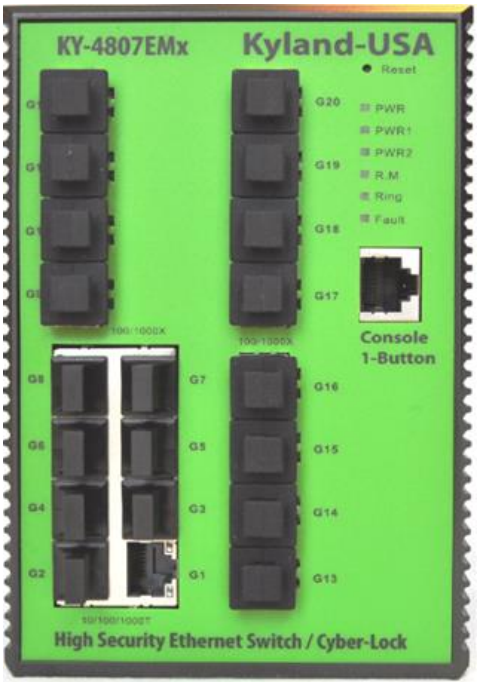


KY-4807EMX

Industrial Managed Gigabit Ethernet Switch

User's Manual

Version 4.0

December, 2014

Compliant: For Military contracts that require the continuous monitoring and protection of industrial control systems (ICS) Networks Operating / monitoring the operating utilities such as Water, Sewer, Electrical, Security, Video, Building Controls, Street and Intelligent Transportation Systems (ITS).

Uses: Cyber-Lock, IP Device Binding, Cyber-Secure Video, Clean Code Technology and IP Source Guard

www.Kyland-USA.com

COPYRIGHT NOTICE

Copyright © 2015 Kyland-USA, LLC.
All rights reserved.
No part of this publication may be reproduced in any form without the prior written consent of Kyland-USA, LLC.

TRADEMARKS

DYMEC is a registered trademark of Kyland-USA, LLC
All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

WARRANTY

Kyland-USA warrants that all Kyland-USA products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). Kyland-USA will repair or replace products found by Kyland-USA to be defective within this warranty period, with shipment expenses apportioned by Kyland-USA and the distributor. This warranty does not cover product modifications or repairs done by persons other than Kyland-USA approved personnel, and this warranty does not apply to Kyland-USA products that are misused, abused, improperly installed, or damaged by accidents.
Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

Information in this publication is intended to be accurate. Kyland-USA shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. Kyland-USA reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

Kyland-USA, LLC
1107 SE Willow Pl, Blue Springs, MO 64014
Telephone: (816) 988-7861
Website: www.Kyland-USA.com

Technical Support
E-mail: Sales@Kyland-USA.com

Sales Contact
E-mail: sales@Kyland-USA.com
training@Kyland-USA (Training)

Table of Content

Getting to Know Your Switch 6
1.1 About the KY-4807EMx Industrial Switch 6
1.2 Software Features 6
1.3 Hardware Features 7

Hardware Installation 8
2.1 Installing Switch on DIN-Rail 8
2.1.1 Mount KY-4807EMX on DIN-Rail 8
2.2 Wall Mounting Installation 9

Hardware Overview 10
3.1 Front Panel 10
3.2 Front Panel LEDs 11
3.3 Top view Panel 12

Cables 13
4.1 Ethernet Cables 13
4.1.1 1000/100BASE-TX/10BASE-T Pin Assignments 13
4.2 SFP 15
4.3 Console Cable 15

WEB Management 16
5.1 Configuration by Web Browser 16
5.1.1 About Web-based Management 16
5.1.2 Basic Setting 18
5.1.2.1 System Information 18
5.1.2.2 Admin&Password 19
5.1.2.3 Auth Method 20
5.1.2.4 IP Setting 21
5.1.2.5 IPv6 Setting ..... **Error! Bookmark not defined.**
5.1.2.6 HTTPS ..... **Error! Bookmark not defined.**
5.1.2.7 SSH ..... **Error! Bookmark not defined.**
5.1.2.8 LLDP 24
5.1.2.9 Modbus TCP ..... **Error! Bookmark not defined.**

5.1.2.10 Backup/Restore Configuration 27
5.1.2.11 Firmware Update 28
5.1.3 DHCP Server 28
5.1.3.1 Setting 28
5.1.3.2 DHCP Dynamic Client List 29
5.1.3.3 DHCP Client List 29
5.1.3.4 DHCP Relay Agent ..... **Error! Bookmark not defined.**
5.1.3.4.1 Relay ..... **Error! Bookmark not defined.**
5.1.3.4.2 Relay Statistics ..... **Error! Bookmark not defined.**
5.1.4 Port Setting 29
5.1.4.1 Port Control 29
5.1.4.2 Port Trunk 31
5.1.4.3 Loop Gourd ..... **Error! Bookmark not defined.**
5.1.5 Redundancy 35
5.1.5.1 MRP ..... **Error! Bookmark not defined.**
5.1.5.2 Ring 35
5.1.5.3 Chain ..... **Error! Bookmark not defined.**
5.1.5.4 MSTP 37
5.1.5.5 Fast Recovery mode ..... **Error! Bookmark not defined.**
5.1.6 VLAN 45
5.1.6.1 VLAN Membership Configuration 45
5.1.6.2 VLAN Port Configuration 46
How is Unaware、C-Port、S-Port、S-Customer Port ? 48
VLAN Setting Example: 52
5.1.6.3 Private VLAN 56
5.1.7 SNMP 58
5.1.7.1 SNMP-System 58
5.1.7.2 SNMP-Communities 60
5.1.7.3 SNMP-Users 61
5.1.7.4 SNMP-Groups 62
5.1.7.5 SNMP-Views 63
5.1.7.6 SNMP-Accesses 64
5.1.8 Traffic Prioritization ..... **Error! Bookmark not defined.**
5.1.8.1 Stom Control ..... **Error! Bookmark not defined.**
5.1.8.2 Port Classifcation ..... **Error! Bookmark not defined.**
5.1.8.3 Port Tag Remaking ..... **Error! Bookmark not defined.**
5.1.8.4 Port DSCP ..... **Error! Bookmark not defined.**

5.1.8.5 Port Policing ..... **Error! Bookmark not defined.**
5.1.8.6 Queue Policing ..... **Error! Bookmark not defined.**
5.1.8.7 QoS Egress Port Scheduler and Shapers ... **Error! Bookmark not defined.**
5.1.8.8 Port Scheduled ..... **Error! Bookmark not defined.**
5.1.8.9 Port Shaping ..... **Error! Bookmark not defined.**
5.1.8.10 DSCP Based QoS ..... **Error! Bookmark not defined.**
5.1.8.11 DSCP Translation ..... **Error! Bookmark not defined.**
5.1.8.12 DSCP Classification ..... **Error! Bookmark not defined.**
5.1.8.13 QoS Control List ..... **Error! Bookmark not defined.**
5.1.8.14 QoS Counters ..... **Error! Bookmark not defined.**
5.1.8.15 QCL Status ..... **Error! Bookmark not defined.**
5.1.9 Multicast ..... **Error! Bookmark not defined.**
5.1.9.1 IGMP Snooping ..... **Error! Bookmark not defined.**
5.1.9.2 IGMP Snooping- VLAN Configuration- ..... **Error! Bookmark not defined.**
5.1.9.3 IGMP Snooping Status ..... **Error! Bookmark not defined.**
5.1.9.4 IGMP Snooping Groups Information ..... **Error! Bookmark not defined.**
5.1.10 Security ..... **Error! Bookmark not defined.**
5.1.10.1 Remote Control Security Configuration ..... **Error! Bookmark not defined.**
5.1.10.2 Device Binding ..... **Error! Bookmark not defined.**
5.1.10.3 ACL ..... **Error! Bookmark not defined.**
5.1.10.4 AAA ..... **Error! Bookmark not defined.**
5.1.10.5 RADIUS Overview ..... **Error! Bookmark not defined.**
RADIUS Authentication Servers ..... **Error! Bookmark not defined.**
RADIUS Accounting Servers ..... **Error! Bookmark not defined.**
5.1.10.6 RADIUS Details ..... **Error! Bookmark not defined.**
5.1.10.7 NAS(802.1x) ..... **Error! Bookmark not defined.**
5.1.11 Warning ..... **Error! Bookmark not defined.**
5.1.11.1 Fault Alarm ..... **Error! Bookmark not defined.**
5.1.11.2 System Warning ..... **Error! Bookmark not defined.**
5.1.12 Monitor and Diag ..... **Error! Bookmark not defined.**
5.1.12.1 MAC Table ..... **Error! Bookmark not defined.**
5.1.12.2 Port Statistic ..... **Error! Bookmark not defined.**
5.1.12.3 Port Mirroring ..... **Error! Bookmark not defined.**
5.1.12.4 System Log Information ..... **Error! Bookmark not defined.**
5.1.12.5 Cable Diagnostics ..... **Error! Bookmark not defined.**
5.1.12.6 SFP Monitor ..... **Error! Bookmark not defined.**
5.1.12.7 Ping ..... **Error! Bookmark not defined.**

5.1.12.8 IPv6 Ping.....**Error! Bookmark not defined.**
5.1.13 Synchronization-PTP.....**Error! Bookmark not defined.**
5.1.14 PoE.....**Error! Bookmark not defined.**
5.1.14.1 Configuration.....**Error! Bookmark not defined.**
5.1.14.2 Status.....**Error! Bookmark not defined.**
5.1.15 Factory Defaults.....**Error! Bookmark not defined.**
5.1.16 System Reboot.....**Error! Bookmark not defined.**

Command Line Interface Management 132
6.1 About CLI Management.....132

Getting to Know Your Switch

1.1 About the KY-4807EMX Industrial Switch

The KY-4807EMX is a managed redundant ring Ethernet switch with 8x10/100/1000Base-T(X) ports and 12x100/1000Base-X SFP ports. The switch supports Ethernet Redundancy protocol, Ring (recovery time < 20ms over 300 units of connection) and MSTP (RSTP/STP compatible). It will protect your mission-critical applications from network interruptions or temporary malfunctions with its fast recovery technology. This unit supports a wide operating temperature from -40 ^{o}C to 85 ^{o}C. The KY-4807EMX can also be managed by Solar Winds, Web-based interface, Telnet and console (CLI) configuration.

Software Features

- Supports Ring (recovery time < 20ms over 300 units of connection) and MSTP(RSTP/STP compatible) for Ethernet Redundancy
- Open-Ring supports non-Kyland-USA vendor's ring technology in an open architecture
- Chain will allow multiple redundant network rings
- Supports IEC 62439-2 MRP (Media Redundancy Protocol) functionality
- Support for IEEE 1588v2 clock synchronization
- Supports IPV6 new internet protocol version
- Support for Modbus TCP protocol
- Supports IEEE 802.3az Energy-Saving Ethernet technology
- Provides HTTPS/SSH protocol to enhance network security
- Supports SMTP client
- Support for IP-based bandwidth management
- Supports application-based QoS management
- Support for Device Binding security function
- Supports DOS/DDOS auto prevention
- IGMP v2/v3 (IGMP snooping support) for filtering multicast traffic
- Supports SNMP v1/v2c/v3 & RMON & 802.1Q VLAN Network Management
- Support for ACL, TACACS+ and 802.1x User Authentication for security
- Supports 9.6K Byte Jumbo Frame
- Multiple notifications for warning of an unexpected event
- Web-based ,Telnet, Console (CLI), and Windows utility (Solar Winds) configuration
- Supports LLDP Protocol
- Rigid IP-30 housing design
- DIN-Rail and wall mounting capable
- Cyber-Secure Video and Clean Code Technology

1.2 Hardware Features

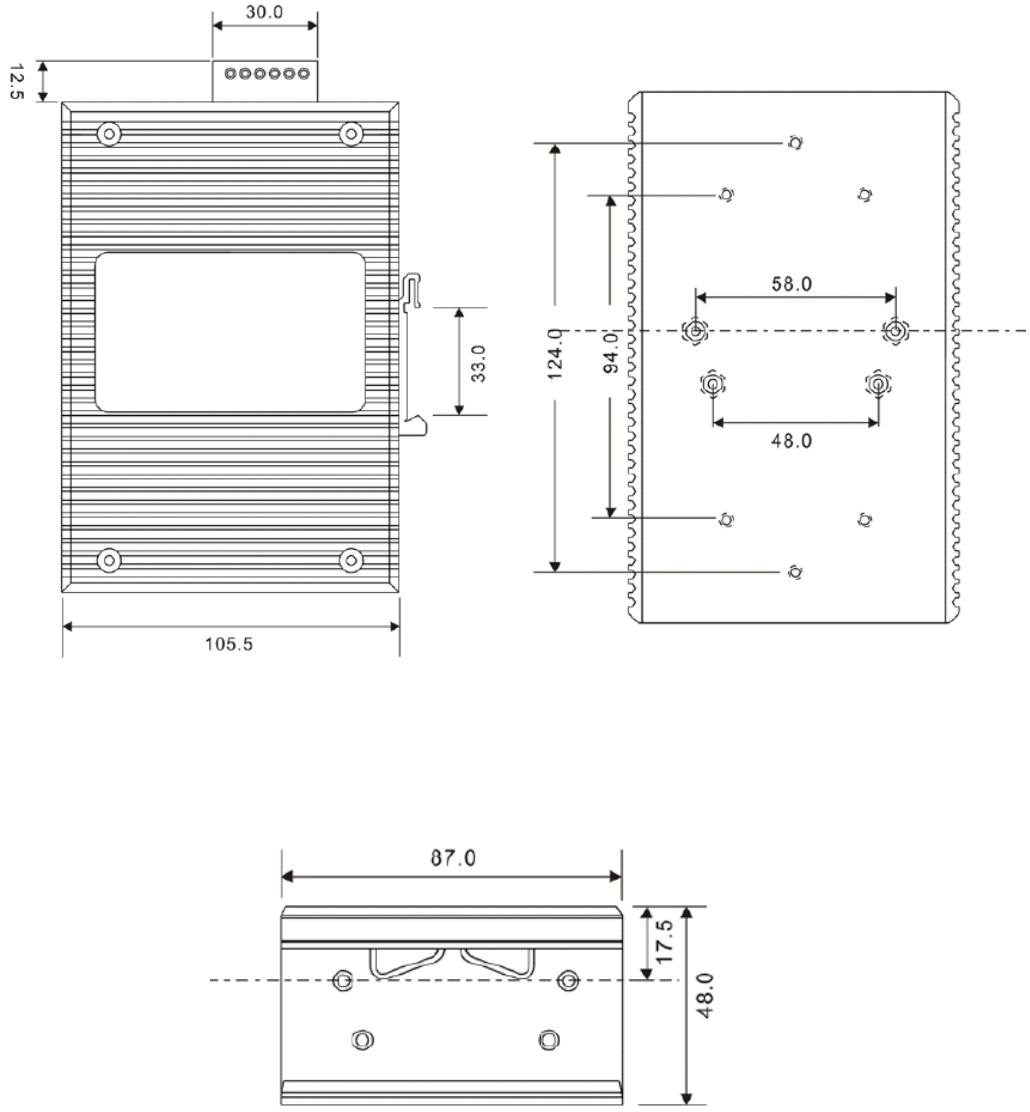
- Redundant DC power inputs
- Operating Temperature: -40 to 85°C
- Storage Temperature: -40 to 85 °C
- Operating Humidity: 5% to 97%, non-condensing
- Casing: IP-30
- 8 x 10/100/1000Base-T(X)
- 12 x 100/1000Base-X with SFP port
- Console Port
- Dimensions 96.4 (W) x 105.5 (D) x 154 (H) mm (3.8 x 4.15 x 6.06 inches)
- IP40 Class Protection

Hardware Installation

2.1 Installing Switch on DIN-Rail

Each switch has a DIN-Rail kit on the rear panel. The DIN-Rail kit helps mount the switch t on the DIN-Rail. It is then easy to install the switch on the DIN-Rail:

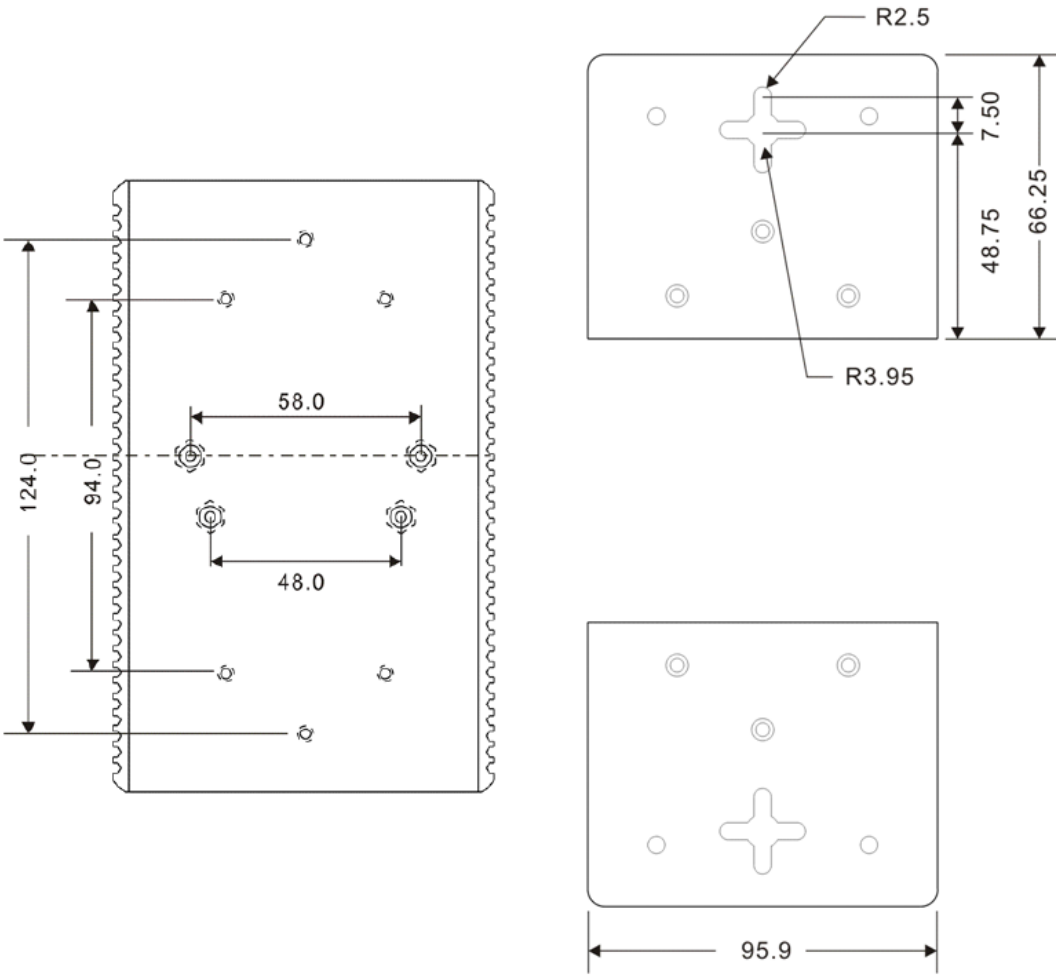
2.1.1 Mount KY-4807EMX on DIN-Rail



DIN-Rail Size

2.2 Wall Mounting Installation

A wall mount panel can also be found in the package. The following steps show how to mount the switch on the wall:



Wall-Mounting size

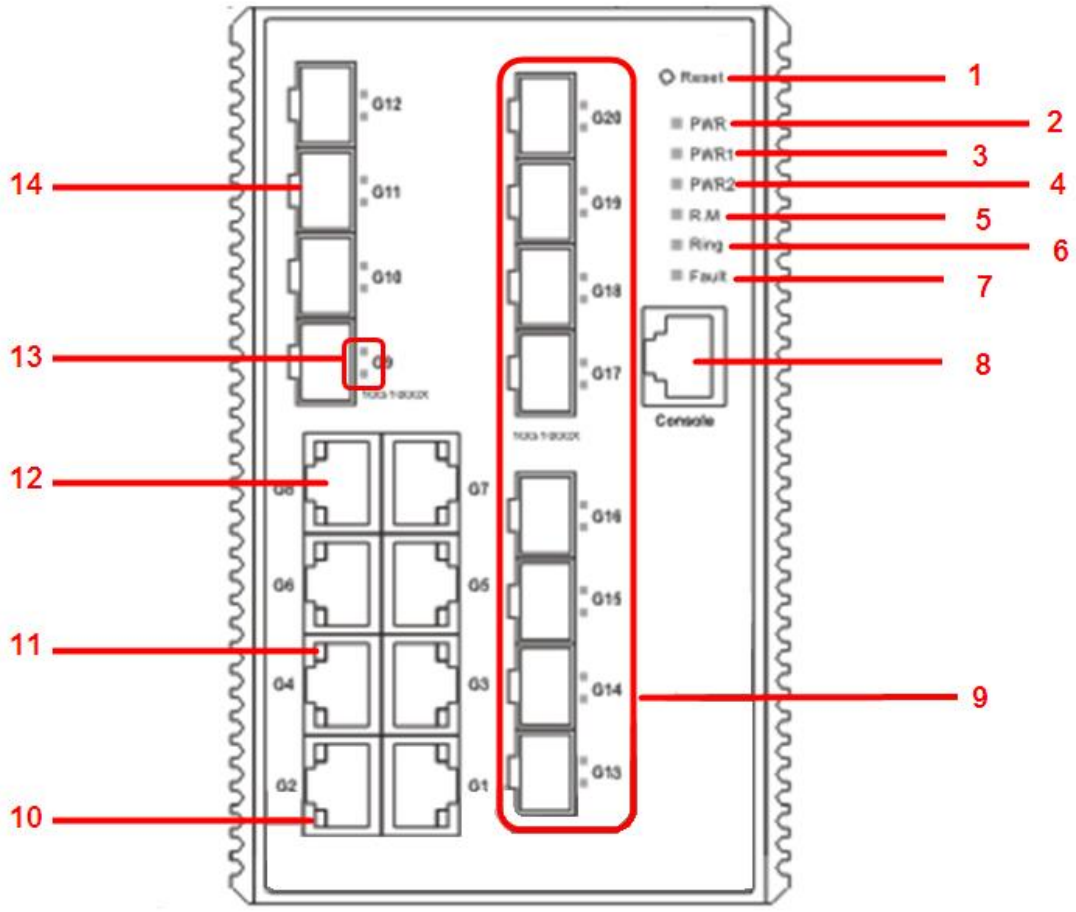
Hardware Overview

3.1 Front Panel

The following table describes the labels that stick on the KY-4807EMX series.

Port	Description
SFP ports	12 100 /1000Base-X
Copper Port	8 10/100/1000Base-T(X)
Console	Use RS-232 with RJ-45 connecter to manage switch.

KY-4807EMX



1. Reset button. Push the button 3 seconds for reset; 5 seconds for factory default.
2. LED for PWR. When the PWR UP, the green led will be light on
3. LED for PWR1
4. LED for PWR2

5. LED for R.M (Ring master). When the LED light on, the switch is the ring master of Ring.，LED for Ring. When the led light is on, the Ring is activated.
6. LED for Ring. When the led light is on, it means that the Ring is activated.
7. LED for Fault. When the light on, it means Power failure or Port down/fail.
8. Console port (RJ-45)
9. 100/1000 Base-X SFP
10. LED for Ethernet ports link status.
11. LED for Ethernet ports speed status
12. 10/100/1000Base-T(X) ports
13. LED for SFP ports link status.
14. 100/1000 Base-X SFP

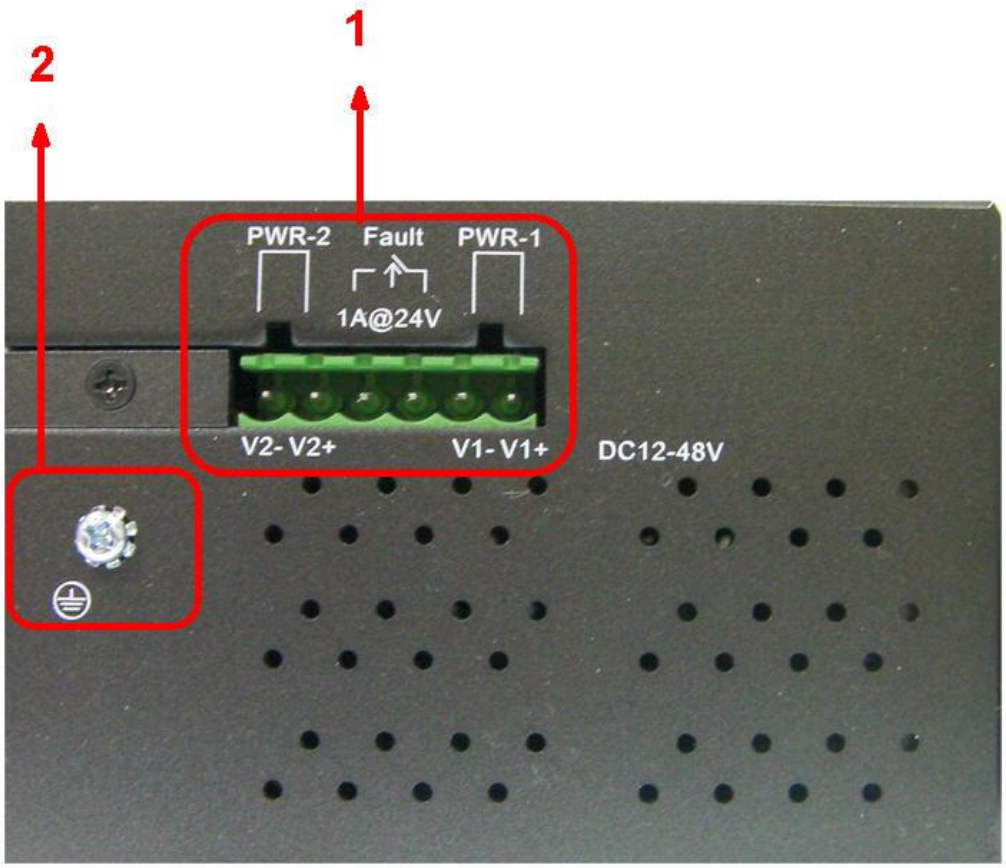
3.2 Front Panel LEDs

LED	Color	Status	Description
PWR	Green	On	DC power module up
PW1	Green	On	DC power module 1activated.
PW2	Green	On	DC Power module 2activated.
R.M	Green	On	Ring Master.
Ring	Green	On	Ring enabled.
		Slowly blinking	Ring has only One link. (Lack of one link to build the ring.)
		Fast blinking	Ring work normally.
Fault	Amber	On	Fault relay. Power failure or Port down/fail.
10/100/1000Base-T(X) Fast Ethernet ports			
LNK	Green	On	Port link up.
ACT	Green	Blinking	Data transmitted.
Full Duplex	Amber	On	Port works under full duplex.
SFP			
LNK	Green	On	Port link up.
ACT	Green	On	Data transmitted.

3.3 Top view Panel

The bottom panel of the KY-4807EMX is shown below:

1. Terminal block includes: PWR1, PWR2 (12-48V DC), Fault Relay
2. Ground wire



.

Cables

4.1 Ethernet Cables

The KY-4807EMX switch has standard Ethernet ports. According to the link type, the switch may use CAT 3, 4, 5,5e, 6 UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45
1000BASE-TX	Cat. 5/Cat. 5e 100-ohm Cat 6 UTP	UTP 100 m (328ft)	RJ-45

4.1.1 1000/100BASE-TX/10BASE-T Pin Assignments

With 1000/100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

10/100 Base-T RJ-45 Pin Assignments

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

1000 Base-T RJ-45 Pin Assignments

Pin Number	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

The KY-4807EMX switch supports auto MDI/MDI-X operation. You can use a straight-through cable to connect PC to switch. The following table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

10/100 Base-T MDI/MDI-X pins assignment

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

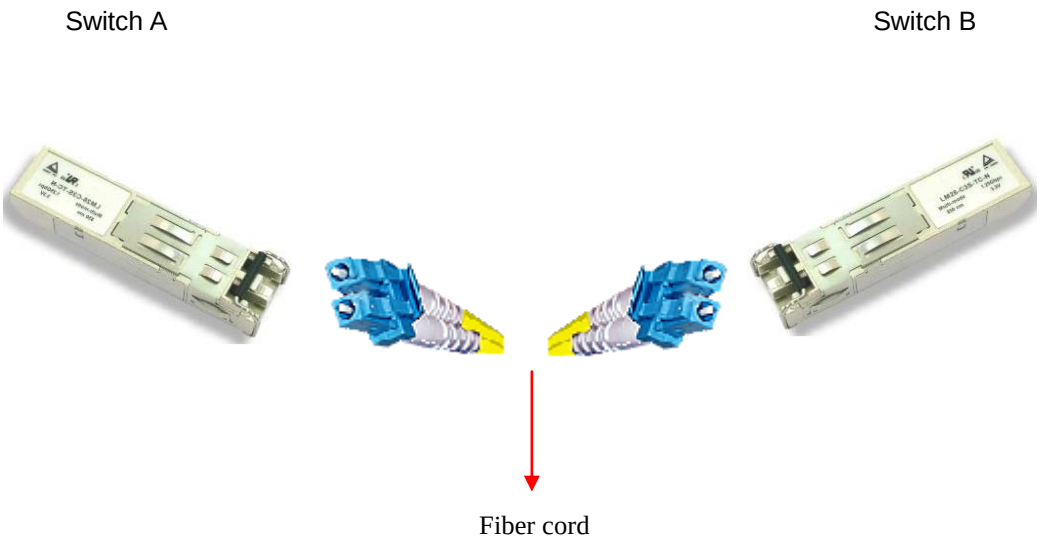
1000 Base-T MDI/MDI-X pins assignment

Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

4.2 SFP

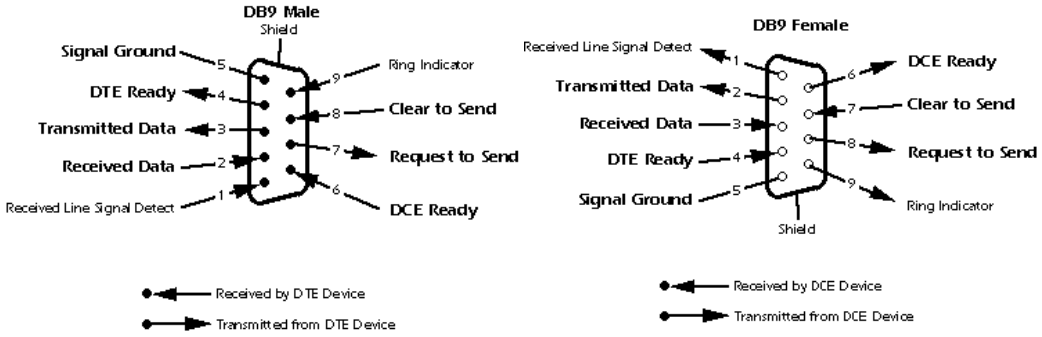
The Switch has fiber optical ports with SFP connectors. The fiber optical ports are in multi-mode (0 to 550M, 850 nm with 50/125 µm, 62.5/125 µm fiber) and single-mode with LC connector. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.



4.3 Console Cable

KY-4807EMX switch can be management by the console port. The DB-9 to RJ-45 cable can be found in the package. You can connect them to PC via a RS-232 cable with DB-9 female connector and the other end (RJ-45 connector) connects to console port of switch.

PC pin out (male) assignment	RS-232 with DB9 female connector	DB9 to RJ 45
Pin #2 RD	Pin #2 TD	Pin #2
Pin #3 TD	Pin #3 RD	Pin #3
Pin #5 GD	Pin #5 GD	Pin #5



WEB Management

Warning!!!
While making any establishment and upgrading firmware, please remove physical loop connection first.
DO NOT power off equipment during firmware is upgrading!

5.1 Configuration by Web Browser

This section introduces the configuration by Web browser.

5.1.1 About Web-based Management

An embedded HTML web site resides in flash memory on the CPU board. It contains advanced management features and allows you to manage the switch from anywhere on the network through a standard web browser such as Microsoft Internet Explorer.

The Web-Based Management function supports Internet Explorer 5.0 or later. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Note: By default, IE5.0 or later version does not allow Java Applets to open sockets. You need to explicitly modify the browser setting in order to enable Java Applets to use network ports.

Preparing for Web Management

The default value is as below:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

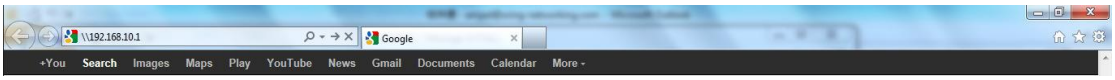
Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

System Login

1. Launch the Internet Explorer.
2. Type http:// and the IP address of the switch. Press "**Enter**".



3. The login screen appears.
4. Key in the username and password. The default username and password is "**admin**".
5. Click "**Enter**" or "**OK**" button, then the main interface of the Web-based management appears.

Login screen

Main Interface

System	
Name	KY-4807EMx
Description	Industrial 20-PORT managed Gigabit Ethernet switch with 8x10/100/1000BASE-T(X) PORTS AND 12x100/1000BASE-X, SFP SOCKET
Location	
Contact	
OID	1.3.6.1.4.1.25972.109.0.0.113
Hardware	
MAC Address	78-ec-74-ff-ff-ff
Time	
System Date	1970-01-01 00:02:22+00:00
System Uptime	0d 00:02:22
Software	
Kernel Version	v9.14
Software Version	v1.00
Software Date	2014-12-02T15:59:00+08:00

Auto-refresh Refresh

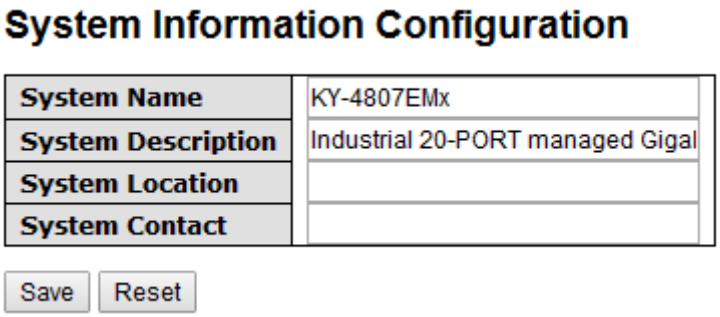
Enable Location Alert

Main interface

5.1.2 Basic Setting

5.1.2.1 System Information

The switch system information is provided here.



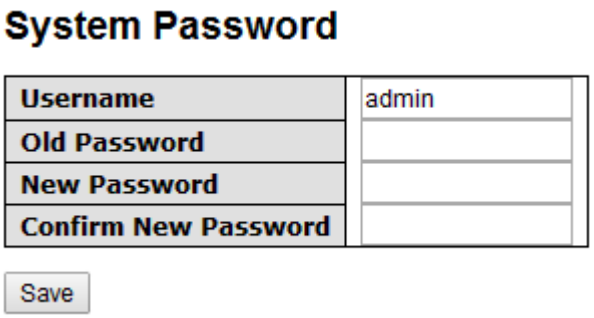
System Information interface

.

Label	Description
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Description	The device Description.
System Location	The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
System Time Zone offset(minutes)	Provide the time-zone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.2.2 Admin & Password

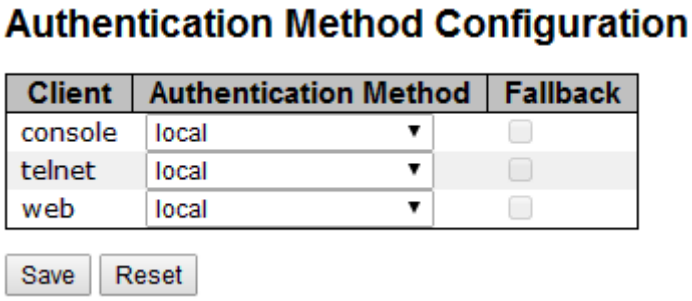
This page allows you to configure the system password required to access the web pages or log in from CLI.



Label	Description
Old Password	Enter the current system password. If this is incorrect, the new password will not be set.
New Password	The system password. The allowed string length is 0 to 31, and the allowed content is the ASCII characters from 32 to 126.
Confirm password	Re-type the new password.
Save	Click to save changes.

5.1.2.3 Authentication Method

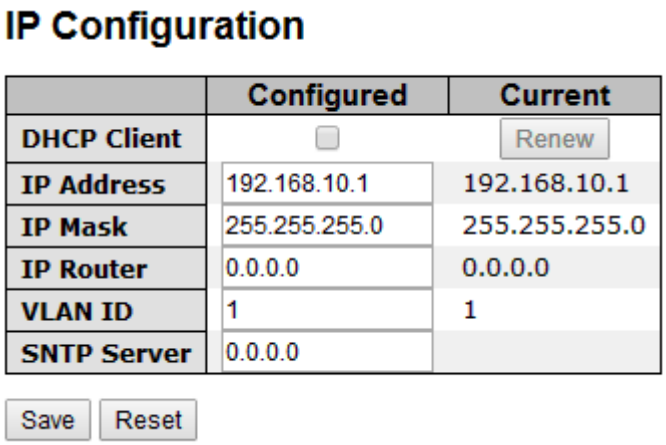
This page allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.



Label	Description
Client	The management client for which the configuration below applies.
Authentication Method	Authentication Method can be set to one of the following values: None: authentication is disabled and login is not possible. Local: use the local user database on the switch for authentication. Radius: use a remote RADIUS server for authentication.
Fallback	Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication. This is only possible if the Authentication Method is set to a value other than 'none' or 'local'.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.2.4 IP Setting

Configure the switch-managed IP information on this page.

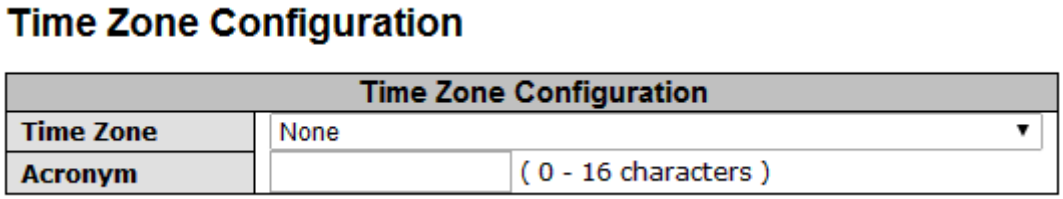


Label	Description
DHCP Client	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
IP Address	Assign the IP address that the network is using. If DHCP client function is enabled, you do not need to assign the IP address. The network DHCP server will assign the IP address for the switch and it will be displayed in this column. The default IP is 192.168.10.1
IP Mask	Assign the subnet mask of the IP address. If DHCP client function is enabling, you do not need to assign the subnet mask
IP Router	Assign the network gateway for the switch. The default gateway is 192.168.10.254
VLAN ID	Provide the managed VLAN ID. The allowed range is 1 through 4095.
DNS Server	Provide the IP address of the DNS Server in dotted decimal notation.
Save	Click to save changes.

Reset	Click to undo any changes made locally and revert to previously saved values.

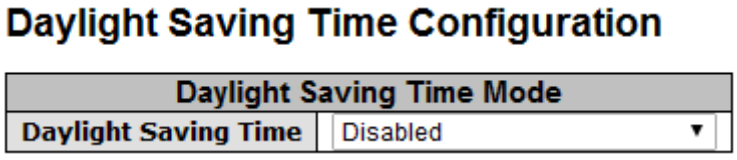
5.1.2.5 Daylight Saving Time

Time Zone Configuration



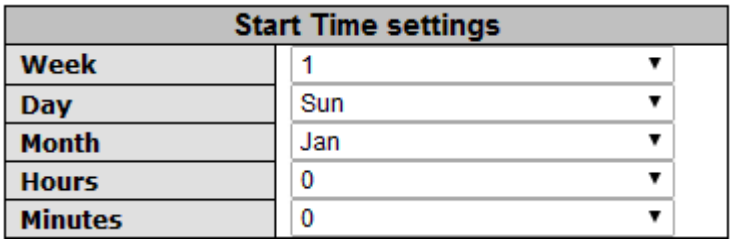
Label	Description
Time Zone	Lists various Time Zones world wide. Select appropriate Time Zone from the drop down and click Save to set.
Acronym	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range: Up to 16 alpha-numeric characters and can contain '-', '_' or '.')

Daylight Saving Time Configuration



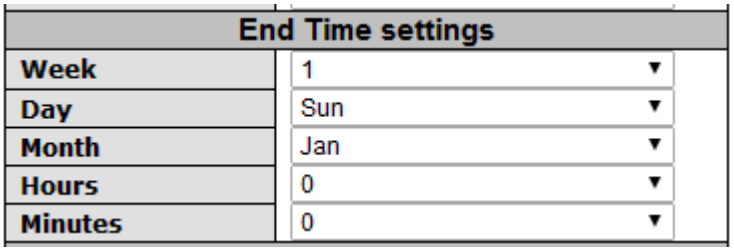
Label	Description
Daylight Saving Time	This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default : Disabled)

Start Time Settings



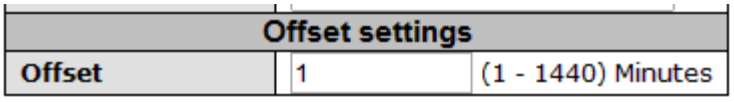
Label	Description
Week	Select the starting week number.
Day	Select the starting day.
Month	Select the starting month.
Hours	Select the starting hour.
Minutes	Select the starting minute.

End Time Settings



Label	Description
Week	Select the ending week number.
Day	Select the ending day.
Month	Select the ending month.
Hours	Select the ending hour.
Minutes	Select the ending minute.

Offset Settings

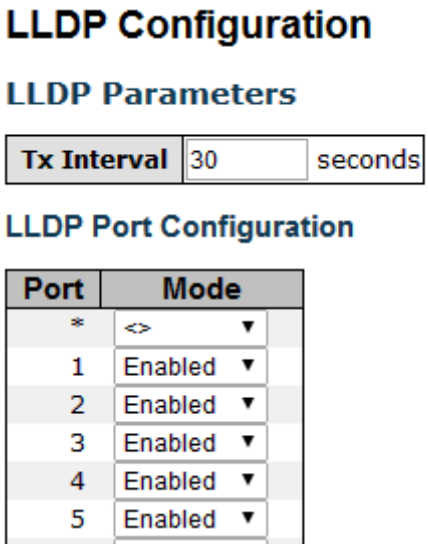


Label	Description
Week	ter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

5.1.2.6 LLDP

LLDP Configuration

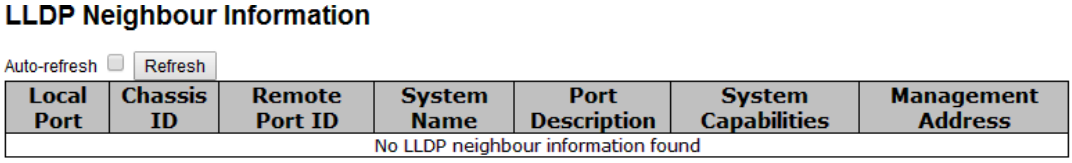
This page allows the user to inspect and configure the current LLDP port settings.



Label	Description
Port	The switch port number of the logical LLDP port.
Mode	Select LLDP mode. Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information. Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors. Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

LLDP Neighbor Information

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:

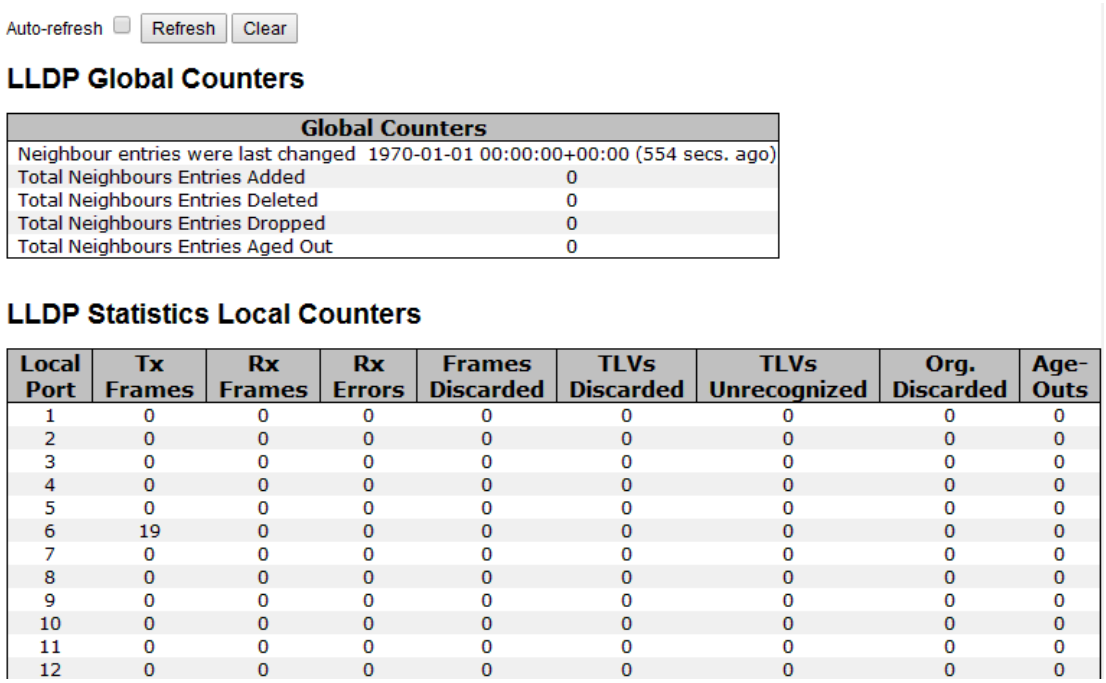


Label	Description
Local Port	The port on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Remote Port ID	The Remote Port ID is the identification of the neighbor port.
System Name	System Name is the name advertised by the neighbor unit.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Capabilities	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
Management Address	Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.
Refresh	Click to refresh the page immediately.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.

Port Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refer to counters for the currently selected switch.


Auto-refresh
Refresh
Clear
LLDP Global Counters
Global Counters
Neighbour entries were last changed 1970-01-01 00:00:00+00:00 (554 secs. ago)
Total Neighbours Entries Added 0
Total Neighbours Entries Deleted 0
Total Neighbours Entries Dropped 0
Total Neighbours Entries Aged Out 0
LLDP Statistics Local Counters
Local Port | Tx Frames | Rx Frames | Rx Errors | Frames Discarded | TLVs Discarded | TLVs Unrecognized | Org. Discarded | Age-Outs
1 0 0 0 0 0 0 0 0
2 0 0 0 0 0 0 0 0
3 0 0 0 0 0 0 0 0
4 0 0 0 0 0 0 0 0
5 0 0 0 0 0 0 0 0
6 19 0 0 0 0 0 0 0
7 0 0 0 0 0 0 0 0
8 0 0 0 0 0 0 0 0
9 0 0 0 0 0 0 0 0
10 0 0 0 0 0 0 0 0
11 0 0 0 0 0 0 0 0
12 0 0 0 0 0 0 0 0

Global Counters

Label	Description
Neighbor entries were last changed at	Shows the time for when the last entry was last deleted or added.
Total Neighbors Entries Added	Shows the number of new entries added since switch reboot.
Total Neighbors Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbors Entries Dropped	Shows the number of LLDP frames dropped due to that the entry table was full.
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

Label	Description
Local Port	The port on which LLDP frames are received or transmitted.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors	The number of received LLDP frames containing some kind of error.
Frames Discarded	If an LLDP frame is received on a port, and the switch's internal

	table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded	The number of organizationally TLVs received.
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.
Refresh	Click to refresh the page immediately.
Clear	Clears the local counters. All counters (including global counters) are cleared upon reboot.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.

5.1.2.7 Backup/Restore Configuration

You can save/view or load the switch configuration. The configuration file is in XML format with a hierarchy of tags:

5.1.2.8 Firmware Update

This page facilitates an update of the firmware controlling the stack. switch.

5.1.3 DHCP Server

5.1.3.1 Setting

The system provides with DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

DHCP Server Configuration

Enabled	☐
Start IP Address	192.168.10.100
End IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Router	192.168.10.254
DNS	192.168.10.254
Lease Time (sec.)	86400
TFTP Server	0.0.0.0
Boot File Name	

Save Reset

5.1.3.2 DHCP Dynamic Client List

When the DHCP server function is activated, the system will collect the DHCP client information and display in here.

DHCP Dynamic Client List

No.	Select	Type	MAC Address	IP Address	Surplus Lease

Select/Clear All | Add to static Table | Delete

5.1.3.3 DHCP Client List

You can assign the specific IP address which is in the assigned dynamic IP range to the specific port. When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before in the connected device.

DHCP Client List

MAC Address	
IP Address	

Add as Static

No.	Select	Type	MAC Address	IP Address	Surplus Lease

Delete | Select/Clear All

5.1.4 Port Setting

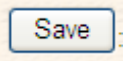
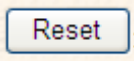
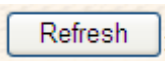
5.1.4.1 Port Control

This page displays current port configurations. Ports can also be configured here.

Port Configuration

Refresh

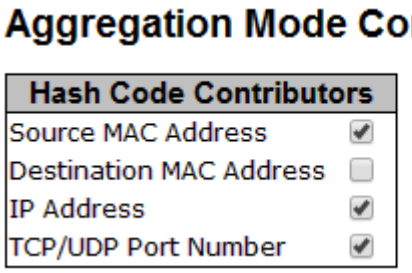
Port	Link	Speed		Flow Control			Maximum Frame Size	Power Control
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>				9600	<>
1		Down	Auto	✗	✗		9600	Disabled
2		Down	Auto	✗	✗		9600	Disabled
3		Down	Auto	✗	✗		9600	Disabled
4		Down	Auto	✗	✗		9600	Disabled
5		Down	Auto	✗	✗		9600	Disabled
6		1Gfdx	Auto	✗	✗		9600	Disabled
7		Down	Auto	✗	✗		9600	Disabled
8		Down	Auto	✗	✗		9600	Disabled
9		Down	Auto	✗	✗		9600	

Label	Description
Port	This is the logical port number for this row.
Link	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
Current Link Speed	Provides the current link speed of the port.
Configured Link Speed	Select any available link speed for the given switch port. Auto Speed selects the highest speed that is compatible with a link partner. Disabled disables the switch port operation. <> : configuration all port .
Flow Control	When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
Maximum Frame	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes.
Power Control	The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port. Disabled: All power savings mechanisms disabled. ActiPHY: Link down power savings enabled. PerfectReach: Link up power savings enabled. Enabled: Both link up and link down power savings enabled.
Total Power Usage	Total power usage in board, measured in percent.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.
	Click to refresh the page. Any changes made locally will be undone.

5.1.4.2 Port Trunk

5.1.4.2.1 Trunk Configuration

This page is used to configure the Aggregation hash mode and the aggregation group.



Label	Description
Source MAC Address	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
Destination MAC Address	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.
IP Address	The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
TCP/UDP Port Number	The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

Aggregation Group Configuration

Group ID	Port Members																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Normal	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
7	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
9	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
10	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Label	Description
Group ID	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

5.1.4.2.2 LACP Port Configuration

This page allows the user to inspect the current LACP port configurations, and possibly change them as well.

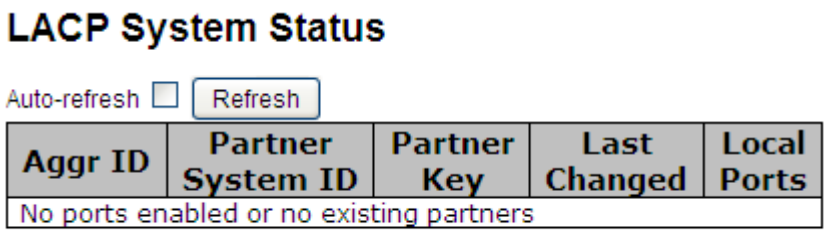
LACP Port Configuration

Port	LACP Enabled	Key		Role
*	☐	<> ▼		<> ▼
1	☐	Auto ▼		Active ▼
2	☐	Auto ▼		Active ▼
3	☐	Auto ▼		Active ▼
4	☐	Auto ▼		Active ▼
5	☐	Auto ▼		Active ▼

Label	Description
Port	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
LACP Enabled	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.
Key	The Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
Role	The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.4.2.3 LACP System Status

This page provides a status overview for all LACP instances.

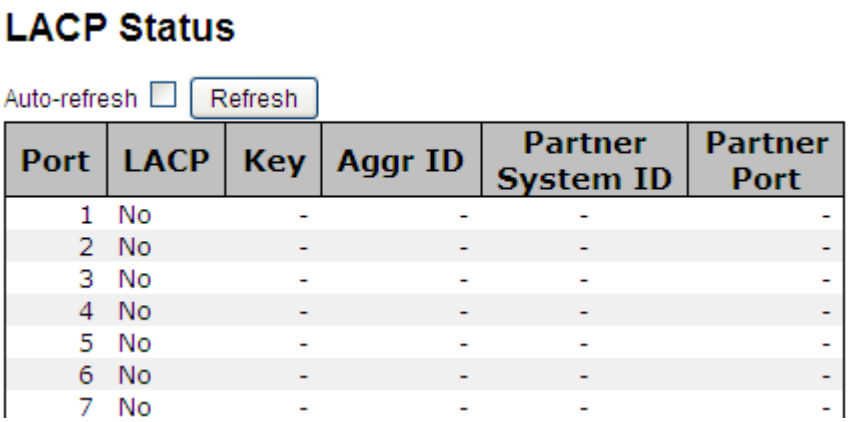


Label	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
Partner System ID	The system ID (MAC address) of the aggregation partner.

Partner Key	The Key that the partner has assigned to this aggregation ID.
Last Changed	The time since this aggregation changed.
Last Changed	Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port".
Refresh	Click to refresh the page immediately.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.

5.1.4.2.4 LACP Status

This page provides a status overview for LACP status for all ports.

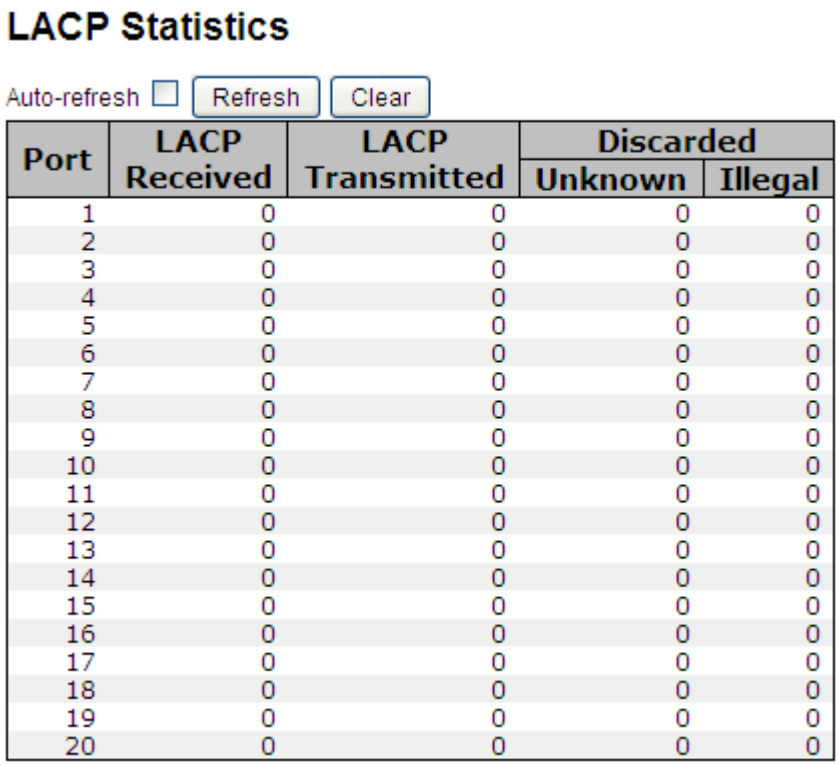


Label	Description
Port	The switch port number.
LACP	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.
Key	The key assigned to this port. Only ports with the same key can aggregate together.
Aggr ID	The Aggregation ID assigned to this aggregation group.
Partner System ID	The partners System ID (MAC address).
Partner Port	The partners' port number connected to this port.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.

5.1.4.2.5 LACP Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refer to counters for the currently selected switch.

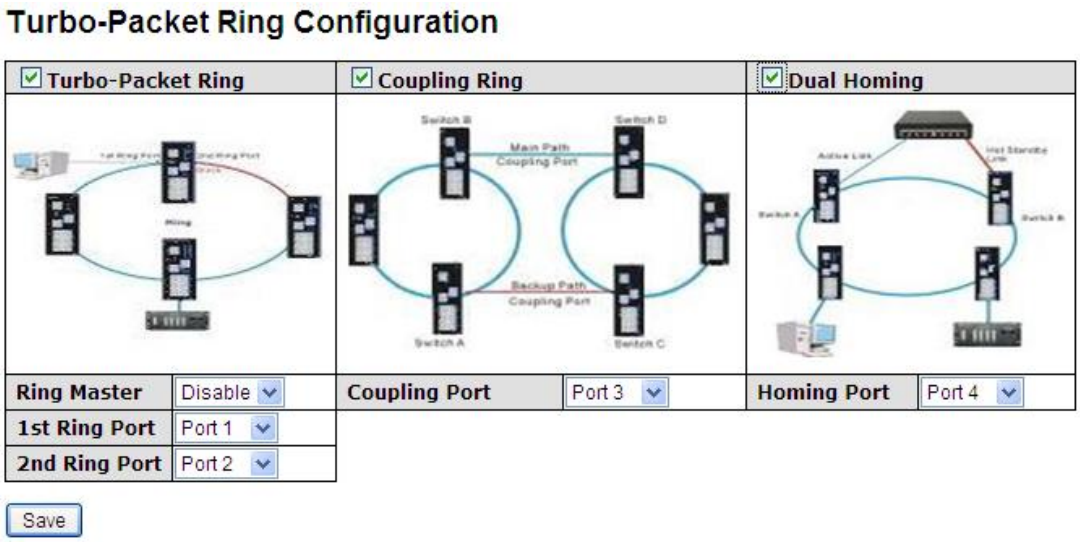


Label	Description
Port	The switch port number
LACP Received	Shows how many LACP frames have been received at each port.
LACP Transmitted	Shows how many LACP frames have been sent from each port.
Discarded	Shows how many unknown or illegal LACP frames have been discarded at each port.

5.1.5 Redundancy

5.1.5.1 Turbo-Packet Ring

Turbo-Packet Ring is the most powerful Ring in the world. The recovery time of Ring is less than 9 ms. It can reduce unexpected damage caused by network topology changes. Ring Supports 3 Ring topologies: **Ring, Coupling Ring and Dual Homing**.



Ring interface

The following table describes the labels in this screen.

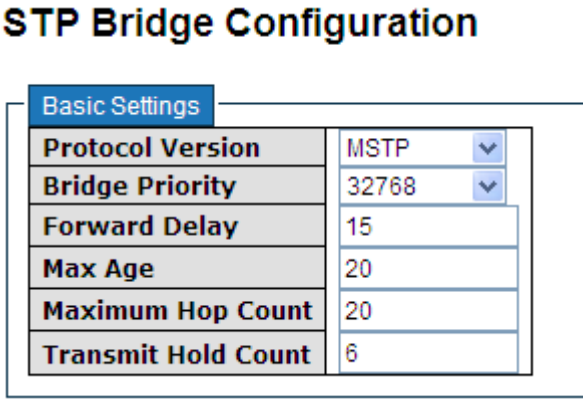
Label	Description
Redundant Ring	Mark to enable Ring.
Ring Master	There should be one and only one Ring Master in a ring. However if there are two or more switches which set Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters.
1st Ring Port	The primary port, when this switch is Ring Master.
2nd Ring Port	The backup port, when this switch is Ring Master.
Coupling Ring	Mark to enable Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller rings to avoid effecting all switches when network topology change. It is a good application for connecting two Rings.
Coupling Port	Link to Coupling Port of the switch in another ring. Coupling Ring need four switch to build an active and a backup link. Set a port as coupling port. The coupled four ports of four switches will be run at active/backup mode.
Dual Homing	Mark to enable Dual Homing. By selecting Dual Homing mode, Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as active/backup mode, and connect each Ring to the normal switches in RSTP mode.
Apply	Click "**Apply**" to set the configurations.

Note: We don't suggest you to set one switch as a Ring Master and a Coupling Ring at the same time due to heavy load.

5.1.5.2 MSTP

Bridge Settings

This page allows you to configure RSTP system settings. The settings are used by all RSTP Bridge instances in the Switch Stack.

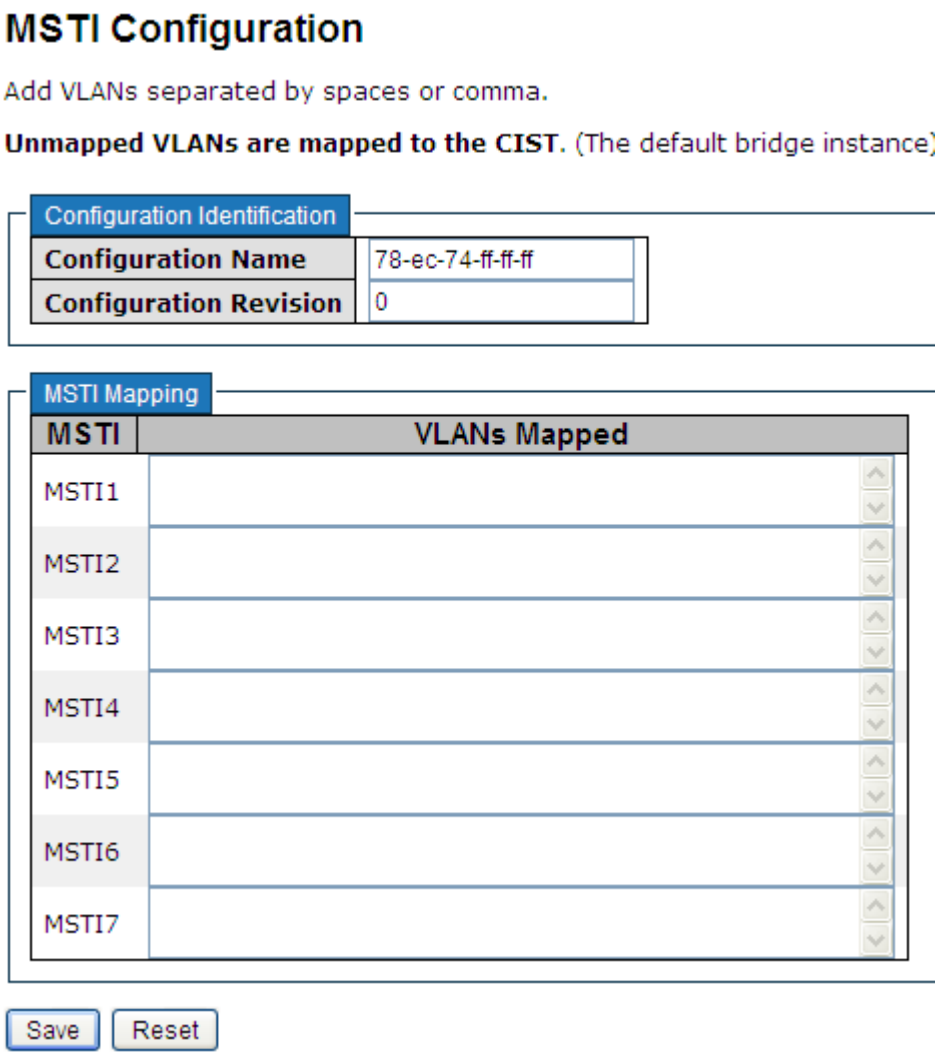


Label	Description
Protocol Version	The STP protocol version setting. Valid values are STP, RSTP and MSTP.
Forward Delay	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.
Maximum Hop Count	This defines the initial value of remainingHops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 4 to 30 seconds, and MaxAge must be <= (FwdDelay-1)*2.
Transmit Hold Count	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

MSTI Mapping

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

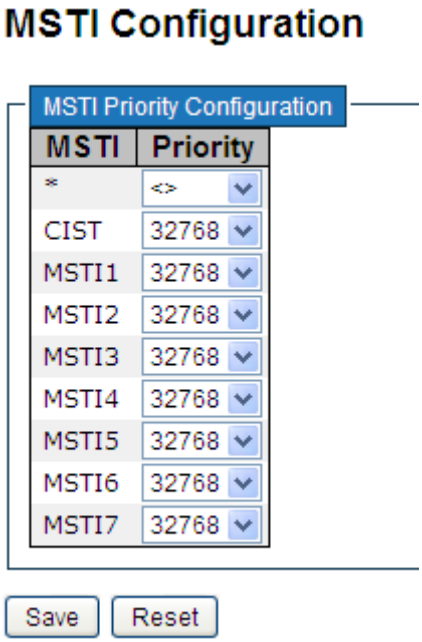


Label	Description
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32

	characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
MSTI	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
VLANS Mapped	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.



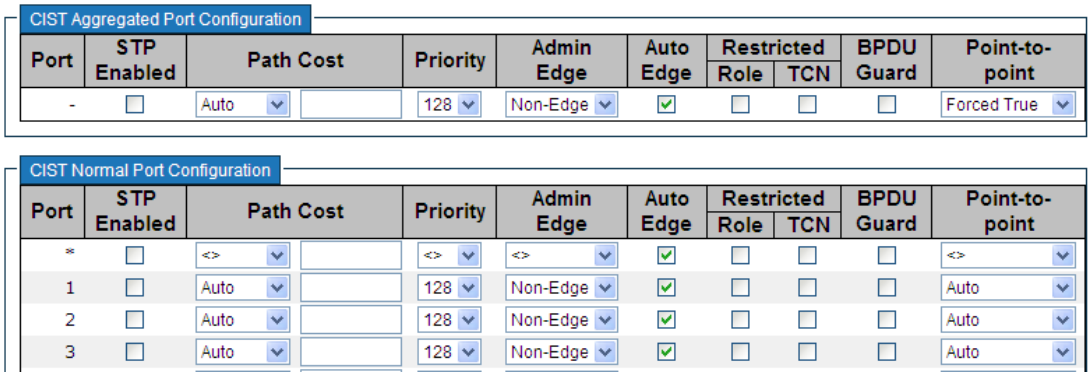
Label	Description
MSTI	The bridge instance. The CIST is the default instance, which is always active.
Priority	Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number,

	concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

CIST Ports

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well. This page contains settings for physical and aggregated ports. The aggregation settings are stack global.

STP CIST Port Configuration



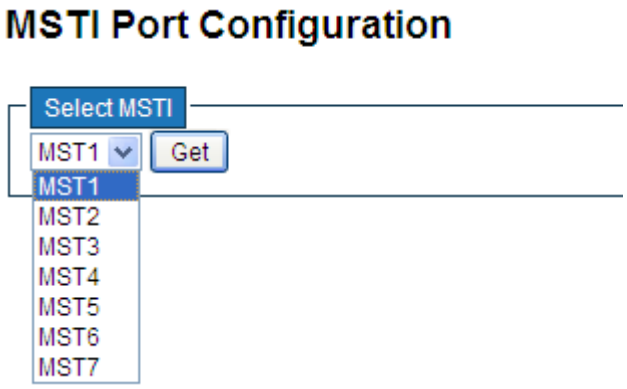
Label	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
OpenEdge (set state flag)	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transitioning to the forwarding state is faster for edge ports (having operEdge true) than for other ports.

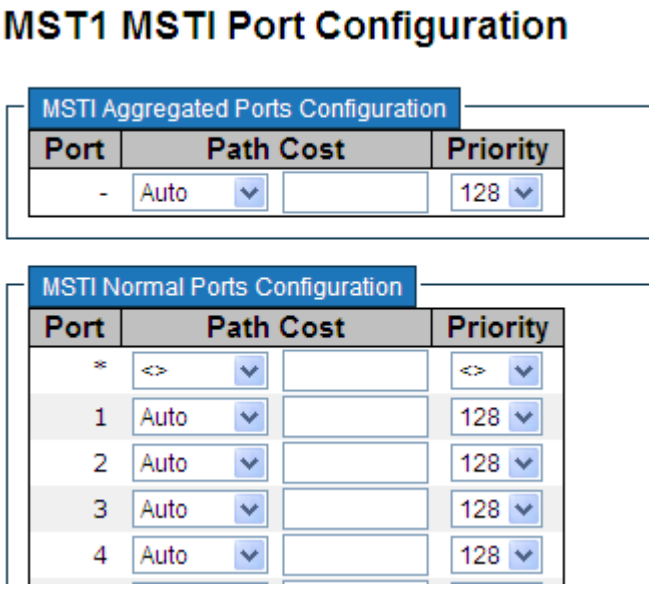
AdminEdge	Controls whether the openEdge flag should start as set or cleared. (The initial openEdge state when a port is initialized).
AutoEdge	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows openEdge to be derived from whether BPDU's are received on the port or not.
Restricted Role	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or is the physical link state for the attached LANs transitions frequently.
Point2Point	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. A MSTI port is a virtual port, which is instantiated seperately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The

MSTI instance must be selected before displaying actual MSTI port configuration options. This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are stack global.





Label	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost

	ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

STP Bridges

This page provides a status overview for all STP bridge instances.

The displayed table contains a row for each STP bridge instance, where the column displays the following information:

STP Bridges

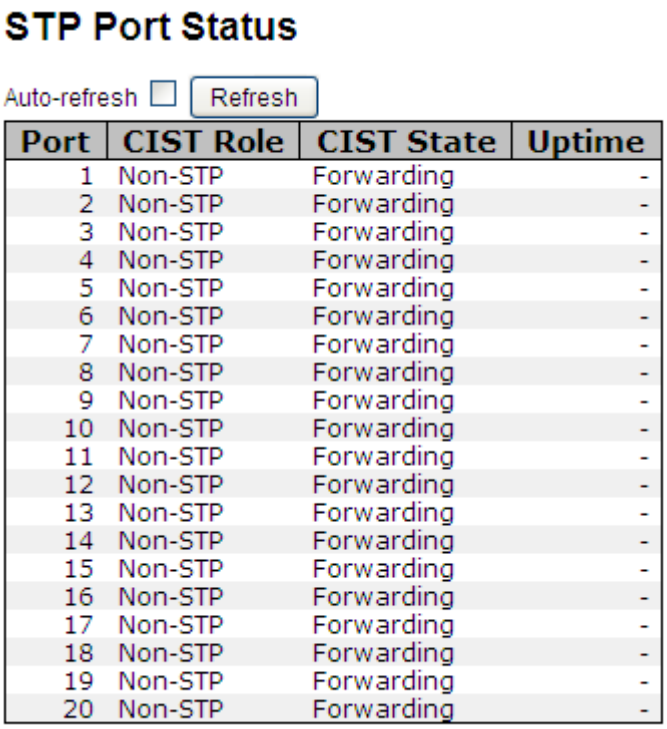
Auto-refresh ☐ Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.78-EC-74-FF-FF-FF	32768.78-EC-74-FF-FF-FF	-	0	Steady	-

Label	Description
MSTI	The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
Bridge ID	The Bridge ID of this Bridge instance.
Root ID	The Bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the root port role.
Root Cost	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Topology Flag	The current state of the Topology Change Flag for this Bridge instance.
Topology Change Last	The time since last Topology Change occurred.
Refresh	Click to refresh the page immediately.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.

STP Port Status

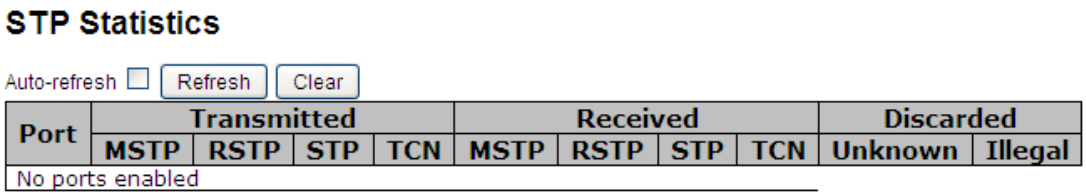
This page displays the STP CIST port status for port physical ports in the currently selected switch.



Label	Description
Port	The switch port number of the logical STP port.
CIST Role	The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort.
State	The current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding.
Uptime	The time since the bridge port was last initialized.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.

STP Statistics

This page displays the RSTP port statistics counters for bridge ports in the currently selected switch.

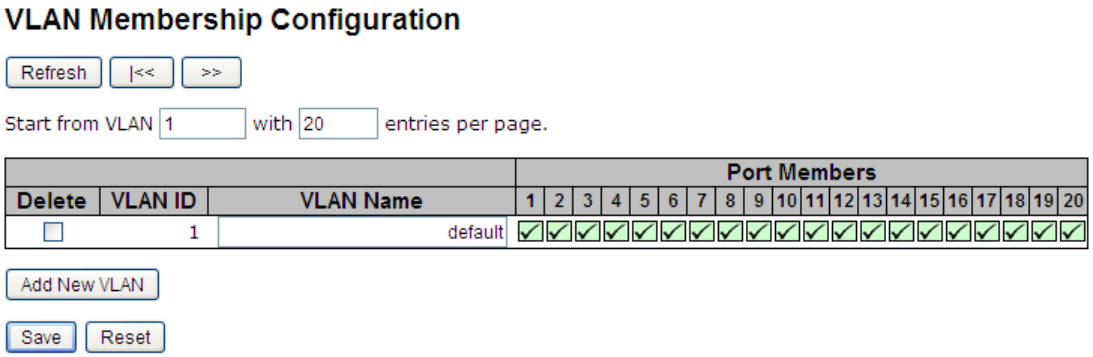


Label	Description
Port	The switch port number of the logical RSTP port.
RSTP	The number of RSTP Configuration BPDU's received/transmitted on the port.
STP	The number of legacy STP Configuration BPDU's received/transmitted on the port.
TCN	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
Discarded Unknown	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
Discarded Illegal	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.

5.1.6 VLAN

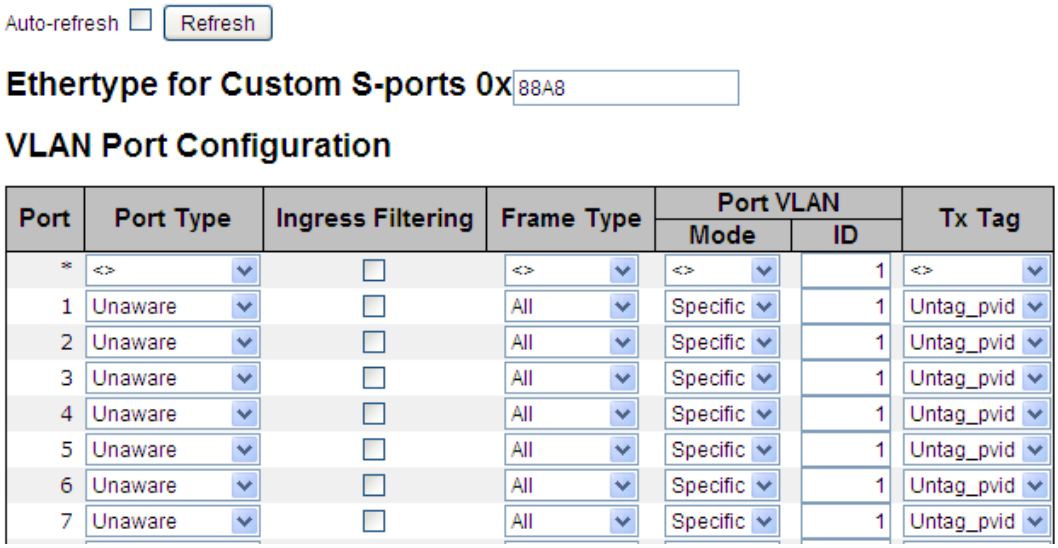
5.1.6.1 VLAN Membership Configuration

The VLAN membership configuration for the selected stack switch unit switch can be monitored and modified here. Up to 64 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New Static Entry	Click Add New VLAN to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The VLAN is enabled on the selected stack switch unit when you click on "Save". The VLAN is thereafter present on the other stack switch units, but with no port members. A VLAN without any port members on any stack unit will be deleted when you click "Save". The Delete button can be used to undo the addition of new VLANs.

5.1.6.2 VLAN Port Configuration



Label	Description
Ethertype for customer S-Ports	This field specifies the ether type used for Custom S-ports. This is a global setting for all the Custom S-ports.
Port	This is the logical port number of this row.
Port type	Port can be one of the following types: Unaware, Customer port(C-port), Service port(S-port), Custom Service port(S-custom-port) If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.
Ingress Filtering	Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).
Frame Type	Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.
Port VLAN Mode	Configures the Port VLAN Mode. The allowed values are None or Specific. This parameter affects VLAN ingress and egress processing. If None is selected, a VLAN tag with the classified VLAN ID is

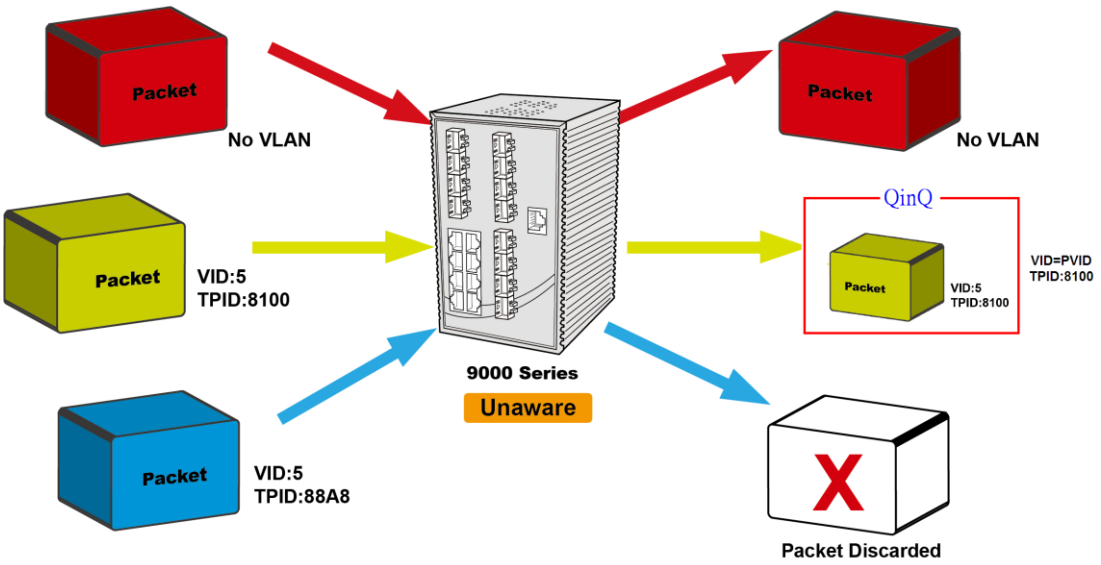
	inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches. Tx tag should be set to Untag_pvid when this mode is used. If Specific (the default value) is selected, a Port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.
Port VLAN ID	Configures the VLAN identifier for the port. The allowed values are from 1 through 4095. The default value is 1. Note: The port must be a member of the same VLAN as the Port VLAN ID.
Tx Tag	Determines egress tagging of a port. Untag_pvid - All VLANs except the configured PVID will be tagged. Tag_all - All VLANs are tagged. Untag_all - All VLANs are untagged.

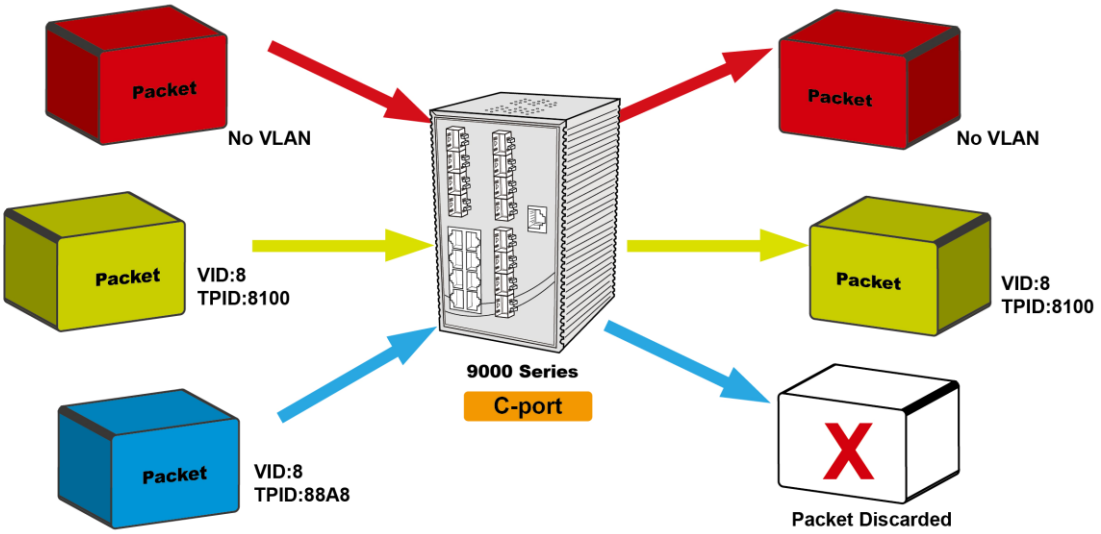
How is Unaware、C-Port、S-Port、S-Customer Port ?

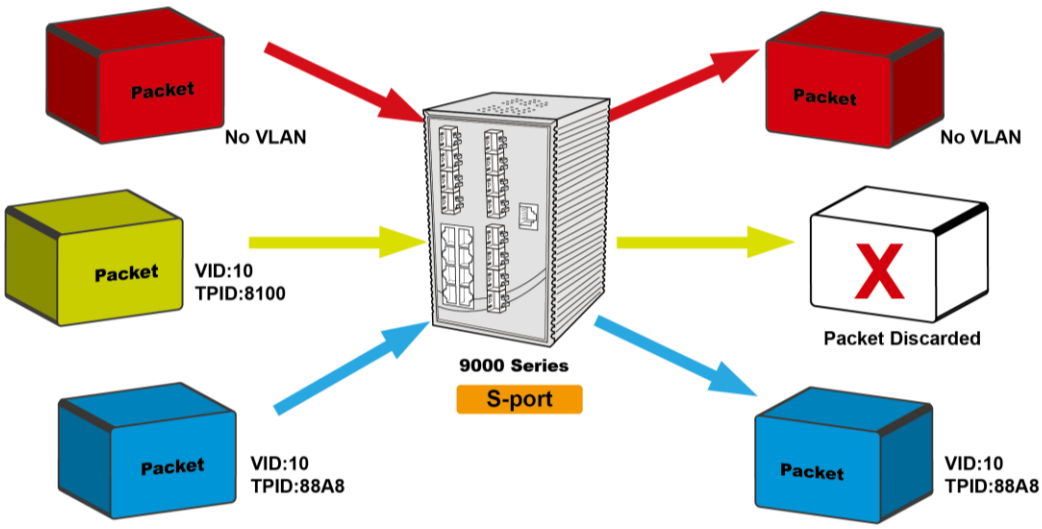
Port can be one of the following types: Unaware, C-port, S-port, and S-custom-port.

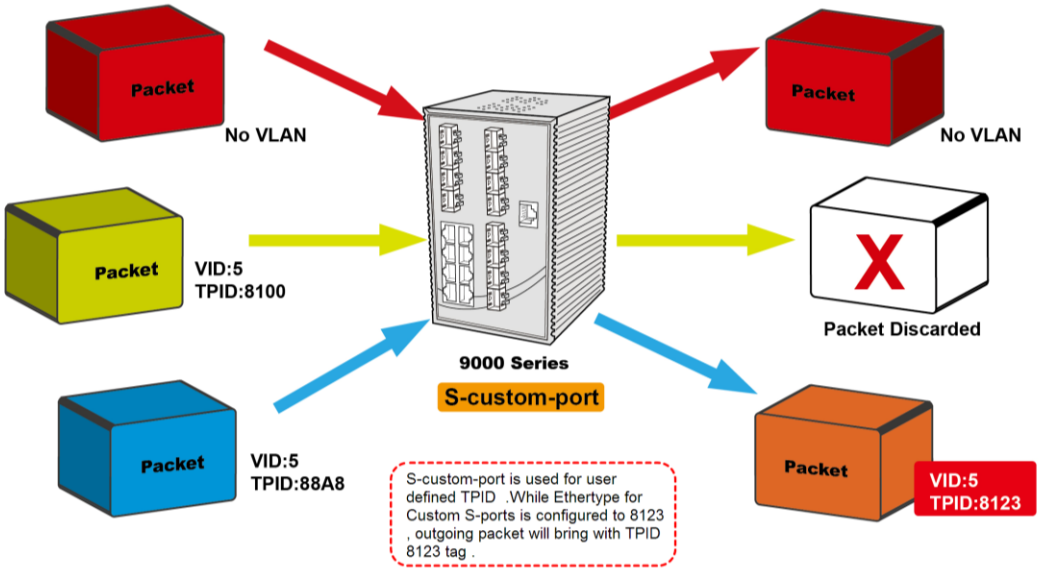
	Ingress action	Egress action
Unaware **The function of Unaware can be used for 802.1QinQ (double tag).**	When the port receives untagged frames, an untagged frame will obtain a tag (based on PVID) and is forwarded. When the port received tagged frames, 1. if the tagged frame with TPID=0x8100, it become a double-tag frame, and is forwarded. 2. if the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by Unaware port will be set to 0x8100. The final status of the frames after egressing are also effected by Egress Rule.
C-port	When the port received untagged frames, an untagged frame obtain a tag (based on PVID) and	The TPID of frame transmitted by C-port

	is forwarded. When the port received tagged frames, 1. if an tagged frame with TPID=0x8100, it is forwarded. 2. if the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	will be set to 0x8100.
S-port	When the port receives untagged frames, an untagged frame will obtain a tag (based on PVID) and is forwarded. When the port received tagged frames, 1. if an tagged frame with TPID=0x88A8, it is forwarded. 2. if the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded.	The TPID of frame transmitted by S-port will be set to 0x88A8.
S-custom-port	When the port receives untagged frames, an untagged frame will obtain a tag (based on PVID) and is forwarded. When the port receives tagged frames, 1. if an tagged frame with TPID=0x88A8, it is forwarded. 2. if the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded.	The TPID of frame transmitted by S-custom-port will be set to a self-customized value, which can be set by the user using the column of **Ethertype for Custom S-ports.**


Packet
No VLAN
Packet
VID:5
TPID:8100
Packet
VID:5
TPID:88A8
9000 Series
Unaware
Packet
No VLAN
QinQ
Packet
VID:5
TPID:8100
VID=PVID
TPID:8100
X
Packet Discarded

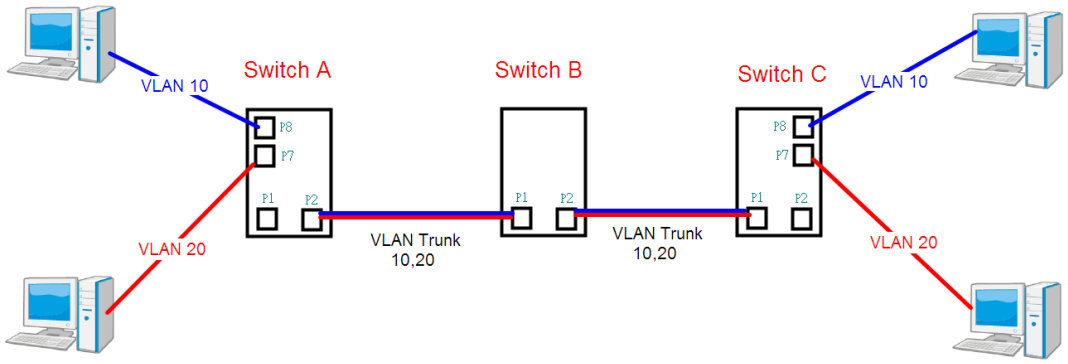

Packet
No VLAN
Packet
VID:8
TPID:8100
Packet
VID:8
TPID:88A8
9000 Series
C-port
Packet
No VLAN
Packet
VID:8
TPID:8100
X
Packet Discarded


Packet
No VLAN
Packet
No VLAN
Packet
VID:10
TPID:8100
X
Packet Discarded
9000 Series
S-port
Packet
VID:10
TPID:88A8
Packet
VID:10
TPID:88A8


Packet
No VLAN
Packet
No VLAN
Packet
VID:5
TPID:8100
X
Packet Discarded
9000 Series
S-custom-port
Packet
VID:5
TPID:88A8
S-custom-port is used for user defined TPID .While Ethertype for Custom S-ports is configured to 8123 , outgoing packet will bring with TPID 8123 tag .
Packet
VID:5
TPID:8123

VLAN Setting Example:

VLAN Access Mode Setting :

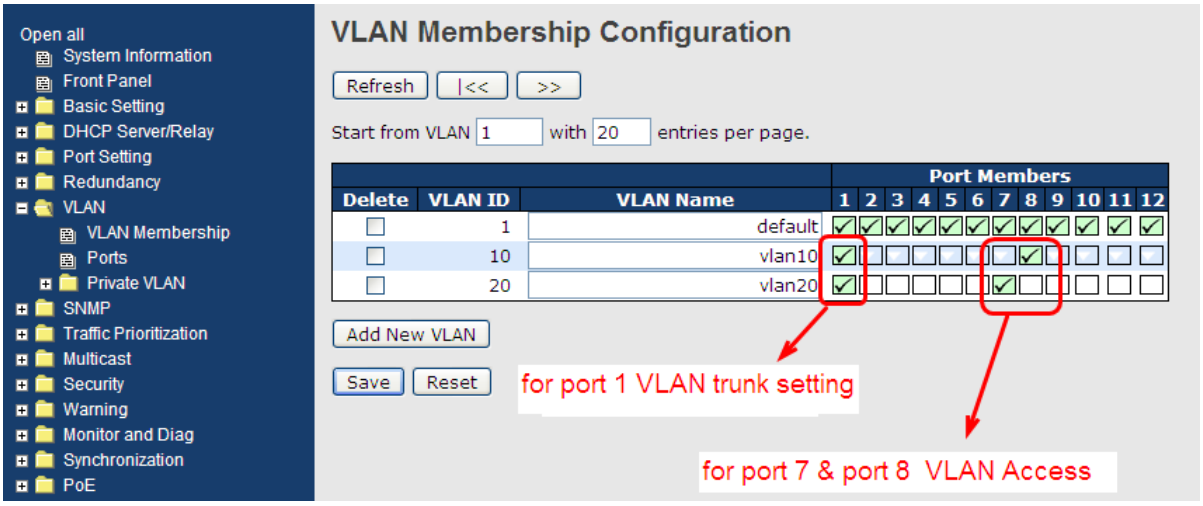


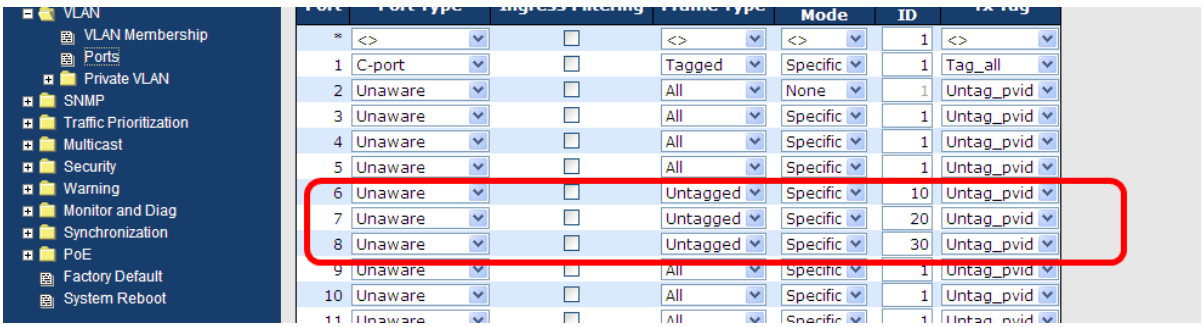
Like this topology, **Switch A**,

Port 7 is VLAN Access mode = Untagged 20

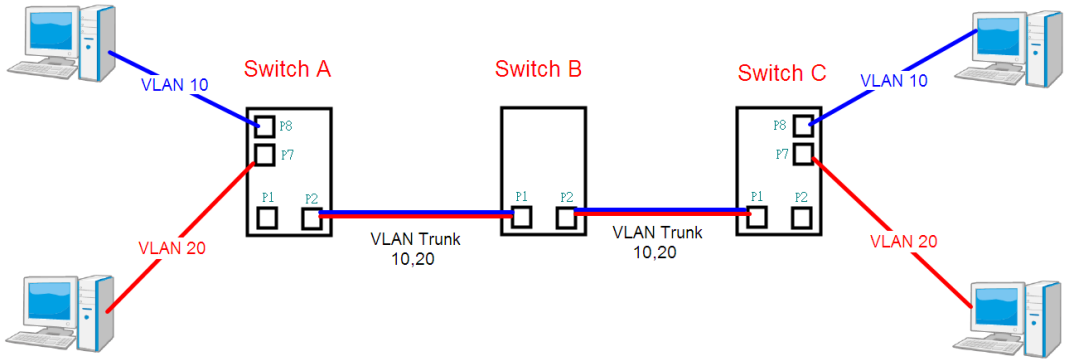
Port 8 is VLAN Access mode = Untagged 10

Switch setting as following





VLAN 1Q Trunk mode :

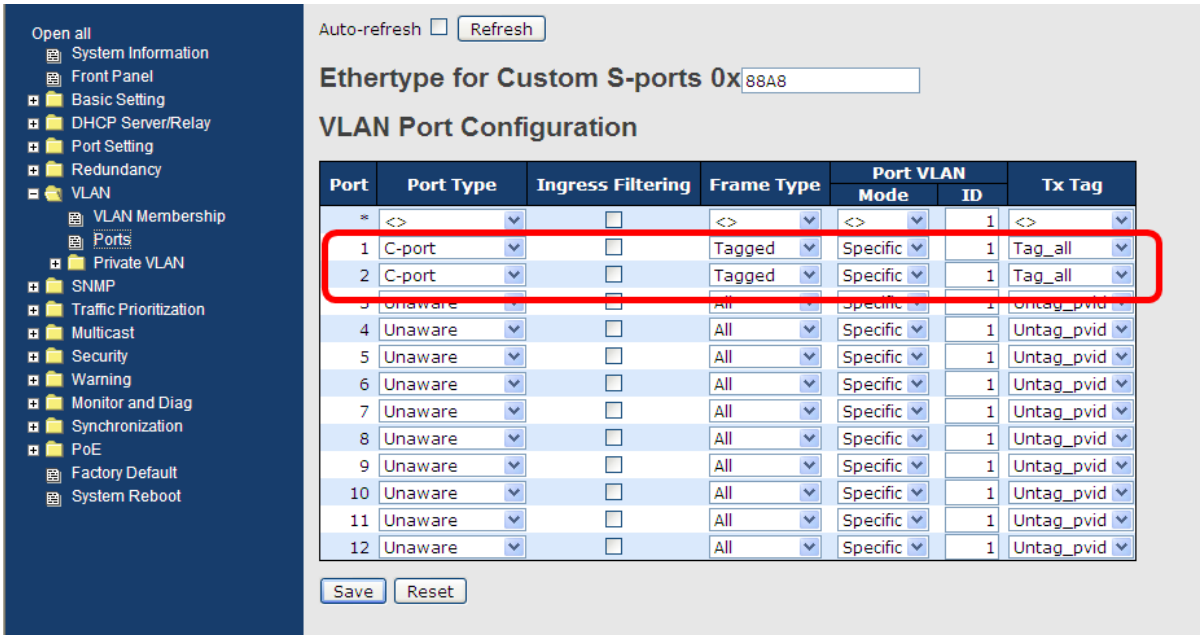


Like this topology, **Switch B**,

Port 1 = VLAN 1Qtrunk mode = tagged 10, 20

Port 2 = VLAN 1Qtrunk mode = tagged 10, 20

Switch setting as following



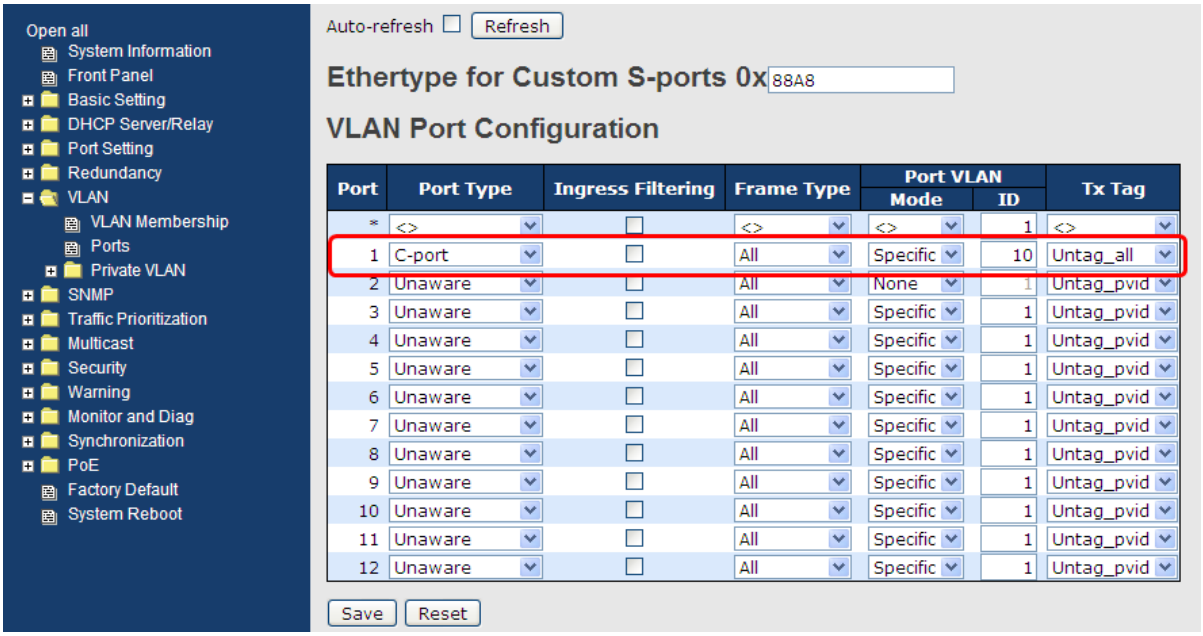
VLAN Hybrid mode:

If user want setting

Port 1 VLAN Hybrid mode = untagged 10

Tagged 10, 20

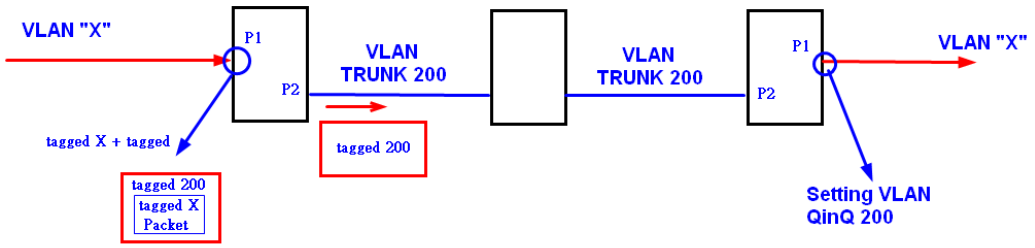
Switch setting as following



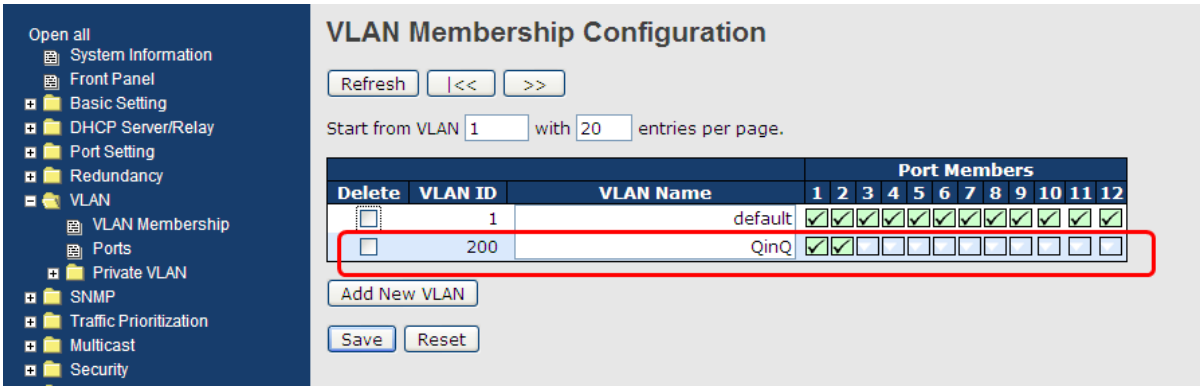
VLAN QinQ mode:

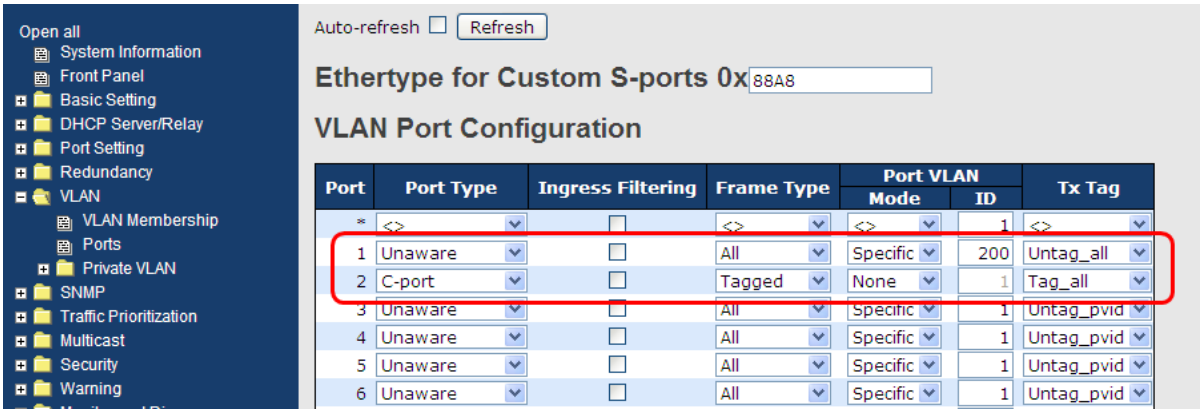
On the VLAN QinQ Mode, usually used in an environment with unknown VLAN, we created a simple example as shown below.

VLAN "X" = Unknown VLAN



KY-4807EMx Series Port 1VLAN Setting

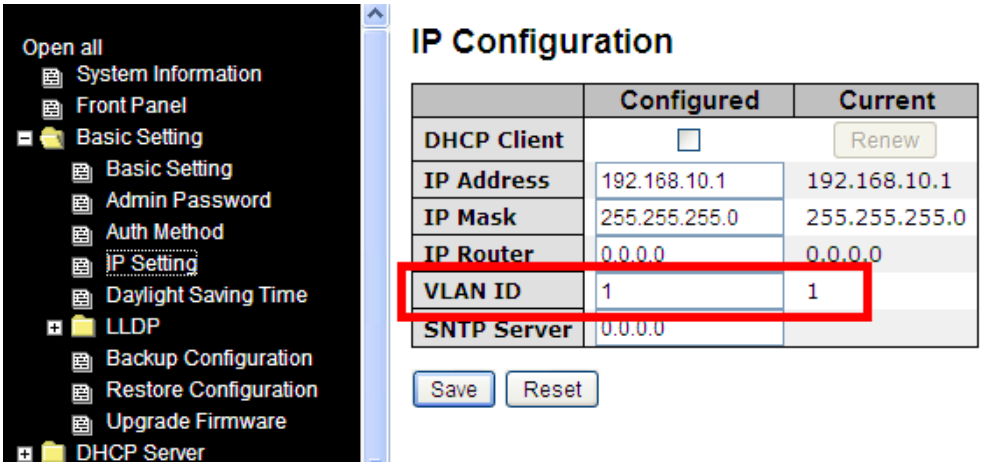




VLAN Management Vlan ID Setting:

If you want to set the Management VLAN, only same VLAN ID port can be used to control the switch.

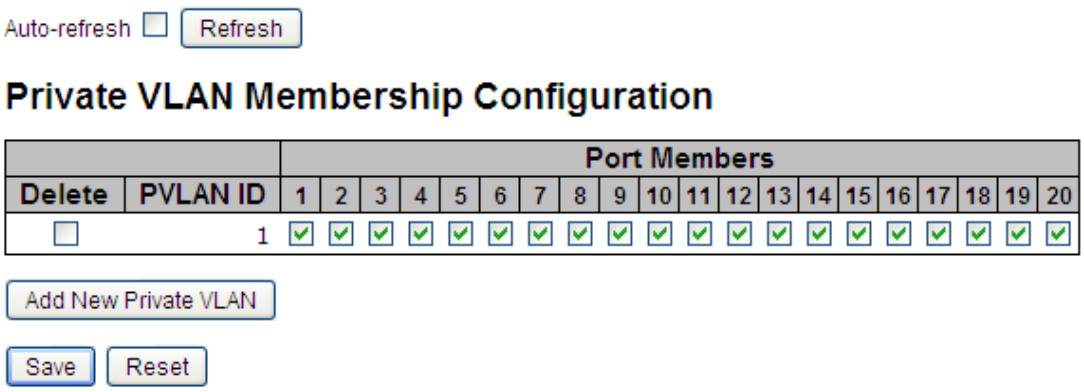
4807EMx Series VLAN Setting



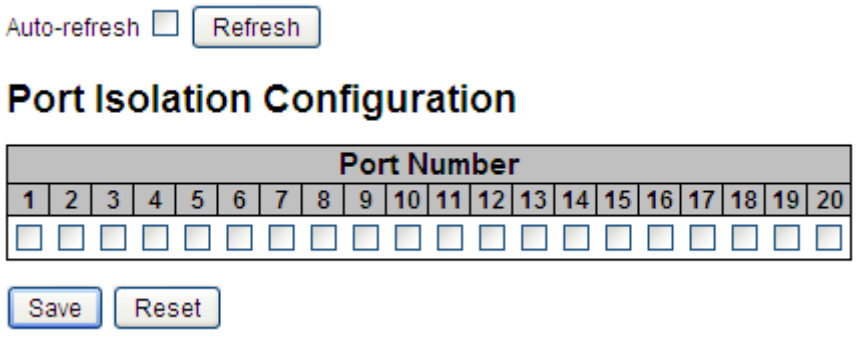
5.1.6.3 Private VLAN

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical. A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.



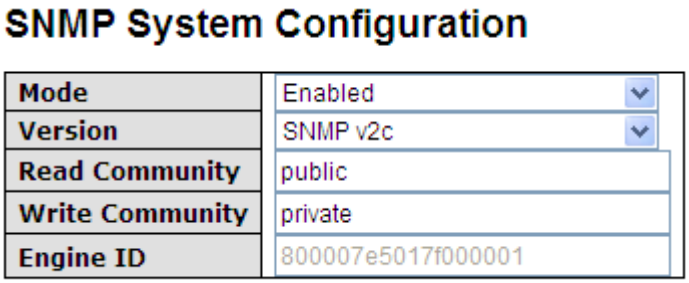
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Private VLAN ID	Indicates the ID of this particular private VLAN.
MAC Address	The MAC address for the entry.
Port Members	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Adding a New Static Entry	Click [Add New Private VLAN] to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction. The Private VLAN is enabled when you click "Save". The [Delete] button can be used to undo the addition of new Private VLANs.



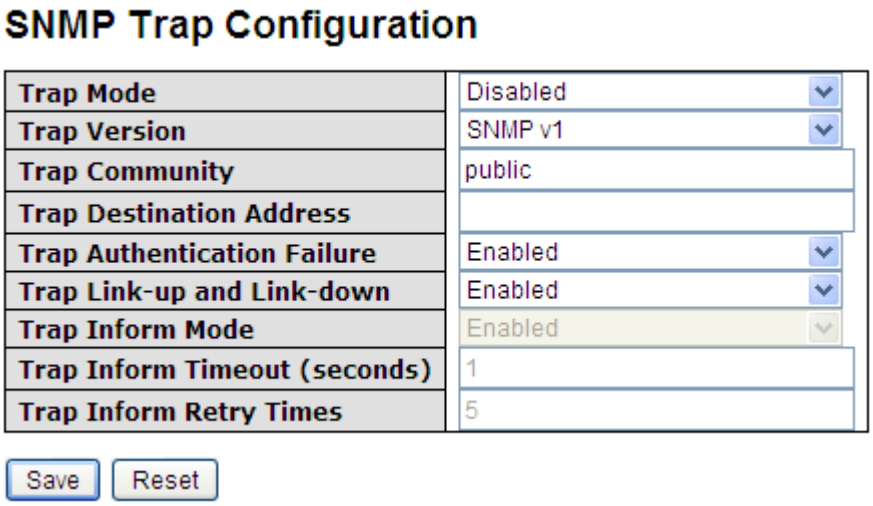
Label	Description
Port Members	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port. By default, port isolation is disabled for all ports.

5.1.7 SNMP

5.1.7.1 SNMP-System



Label	Description
Mode	Indicates the SNMP mode operation. Possible modes are: Enabled: Enable SNMP mode operation. Disabled: Disable SNMP mode operation.
Version	Indicates the SNMP supported version. Possible versions are: SNMP v1: Set SNMP supported version 1. SNMP v2c: Set SNMP supported version 2c. SNMP v3: Set SNMP supported version 3.
Read Community	Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associated with SNMPv3 communities table
Write Community	Indicates the community writes access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associated with SNMPv3 communities table.
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.



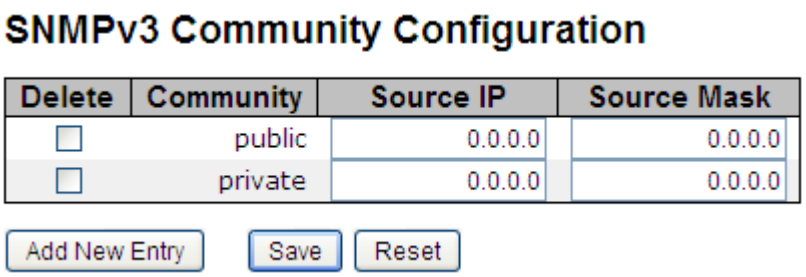
Label	Description
Trap Mode	Indicates the SNMP trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap supported version. Possible versions are: SNMP v1: Set SNMP trap supported version 1. SNMP v2c: Set SNMP trap supported version 2c. SNMP v3: Set SNMP trap supported version 3.
Trap Community	Indicates the community access string when send SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.
Trap Destination Address	Indicates the SNMP trap destination address. Trap Destination IPv6 Address
Trap Destination IPv6 Address	Provide the trap destination IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separate each field (:). For example, 'fe80:215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example, '::192.1.2.34'.
Trap Authentication Failure	Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes are: Enabled: Enable SNMP trap authentication failure. Disabled: Disable SNMP trap authentication failure.
Trap Link-up and	Indicates the SNMP trap link-up and link-down mode operation.

Link-down	Possible modes are: Enabled: Enable SNMP trap link-up and link-down mode operation. Disabled: Disable SNMP trap link-up and link-down mode operation.
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: Enabled: Enable SNMP trap inform mode operation. Disabled: Disable SNMP trap inform mode operation.
Trap Inform Timeout(seconds)	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
Trap Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.
Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.

Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

5.1.7.2 SNMP-Communities

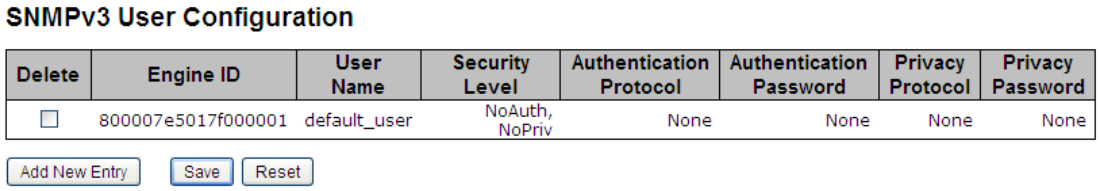
Configure SNMPv3 communities table on this page. The entry index key is Community.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Community	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Source IP	Indicates the SNMP access source address.
Source Mask	Indicates the SNMP access source address mask.

5.1.7.3 SNMP-Users

Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name.

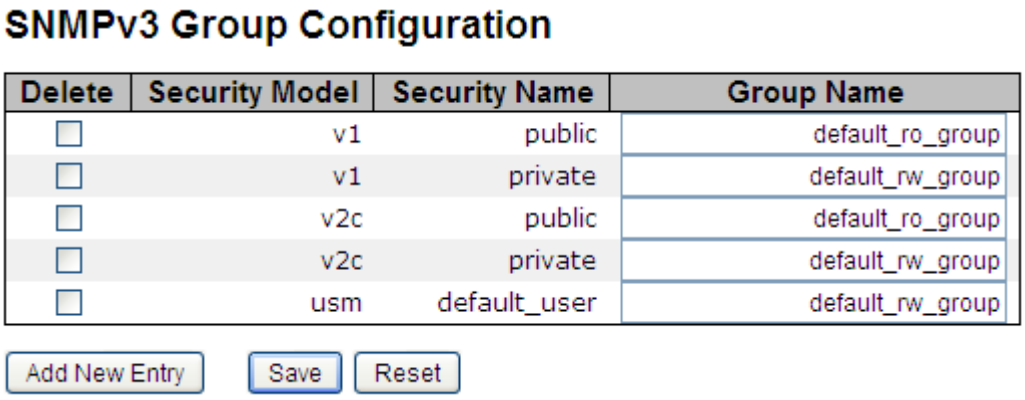


Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote

	SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: None authentication and none privacy. Auth, NoPriv: Authentication and none privacy. Auth, Priv: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: None: None authentication protocol. MD5: An optional flag to indicate that this user using MD5 authentication protocol. SHA: An optional flag to indicate that this user using SHA authentication protocol. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Password	A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is the ASCII characters from 33 to 126.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: None: None privacy protocol. DES: An optional flag to indicate that this user using DES authentication protocol.
Privacy Password	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

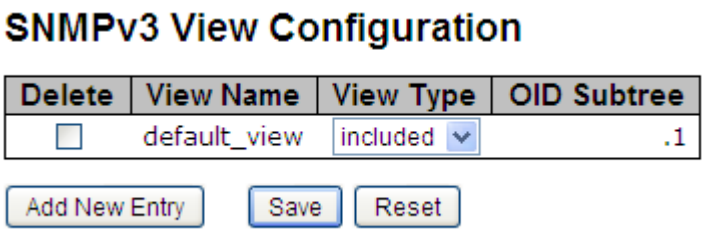
5.1.7.4 SNMP-Groups

Configure SNMPv3 groups table on this page. The entry index keys are Security Model and Security Name.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM).
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

5.1.7.5 SNMP-Views



Label	Description

Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Possible view types are: Included: An optional flag to indicate that this view subtree should be included. Excluded: An optional flag to indicate that this view subtree should be excluded. General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (*).

5.1.7.6 SNMP-Accesses

Configure SNMPv3 accesses table on this page. The entry index keys are Group Name, Security Model and Security Level.

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	default_ro_group	any	NoAuth, NoPriv	default_view	None
☐	default_rw_group	any	NoAuth, NoPriv	default_view	default_view

Add New Entry | Save | Reset

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: Any: Accepted any security model (v1|v2c|usm). v1: Reserved for SNMPv1.

	v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: None authentication and none privacy. Auth, NoPriv: Authentication and none privacy. Auth, Priv: Authentication and privacy.
Read View Name	The name of the MIB views defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Write View Name	The name of the MIB views defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

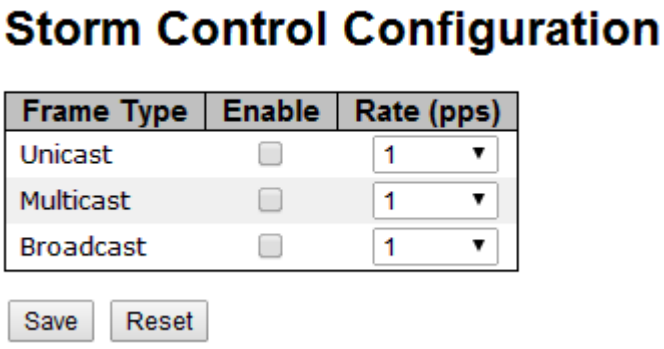
5.1.8 Traffic Prioritization

5.1.8.1 Storm Control

There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

The rate is 2^n, where n is equal to or less than 15, or "No Limit". The unit of the rate can be either pps (packets per second) or kpps (kilo packets per second). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

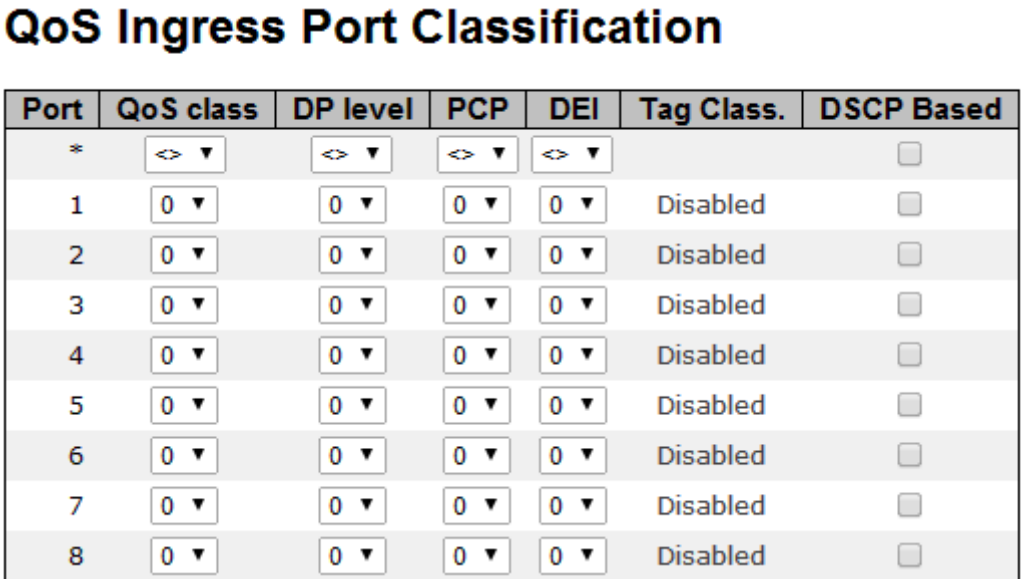
Note: Frames, which are sent to the CPU of the switch, are always limited to approximately 4 kpps. For example, broadcasts in the management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.



Label	Description
Frame Type	The settings in a particular row apply to the frame type listed here: unicast, multicast, or broadcast.
Status	Enable or disable the storm control status for the given frame type.
Rate	The rate unit is packet per second (pps), configure the rate as 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

5.1.8.2 Port Classification

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.



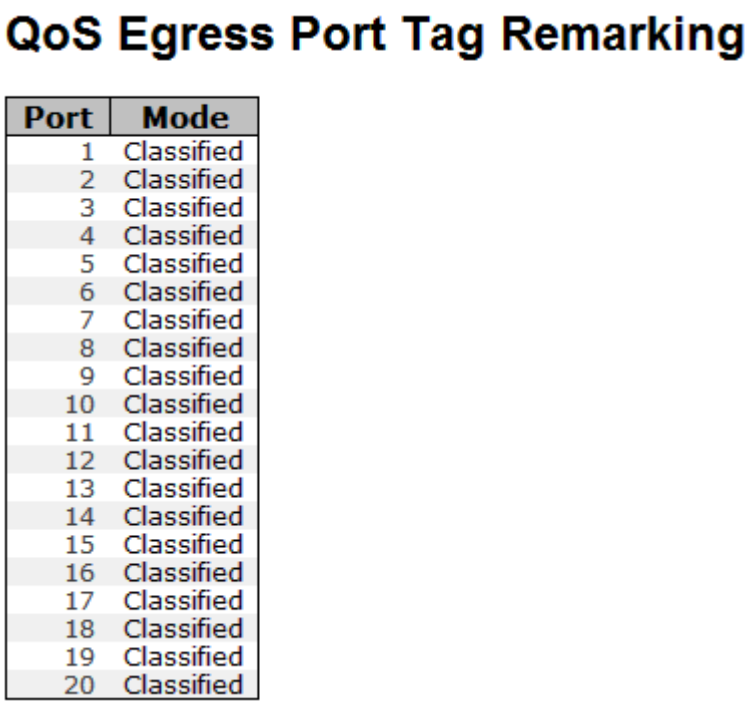
Label	Description
Port	The port number for which the configuration below applies
QoS Class	Controls the default QoS class. All frames are classified to a QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0

	(zero) has the lowest priority. If the port is VLAN aware and the frame is tagged, then the frame is classified to a QoS class that is based on the PCP value in the tag as shown below. Otherwise the frame is classified to the default QoS class. PCP value: 0 1 2 3 4 5 6 7 QoS class: 1 0 2 3 4 5 6 7 If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a QoS class that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default QoS class. The classified QoS class can be overruled by a QCL entry. Note: If the default QoS class has been dynamically changed, then the actual default QoS class is shown in parentheses after the configured default QoS class.
DP level	Controls the default Drop Precedence Level. All frames are classified to a DP level. If the port is VLAN aware and the frame is tagged, then the frame is classified to a DP level that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DP level. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DP level that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DP level. The classified DP level can be overruled by a QCL entry.
PCP	Controls the default PCP value. All frames are classified to a PCP value.

	If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
DEI	Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
Tag Class	Shows the classification mode for tagged frames on this port. Disabled: Use default QoS class and DP level for tagged frames. Enabled: Use mapped versions of PCP and DEI for tagged frames. Click on the mode in order to configure the mode and/or mapping. Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default QoS class and DP level.
DSCP Based	Click to Enable DSCP Based QoS Ingress Port Classification.

5.1.8.3 Port Tag Remaking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.



QoS Egress Port Tag Remarking

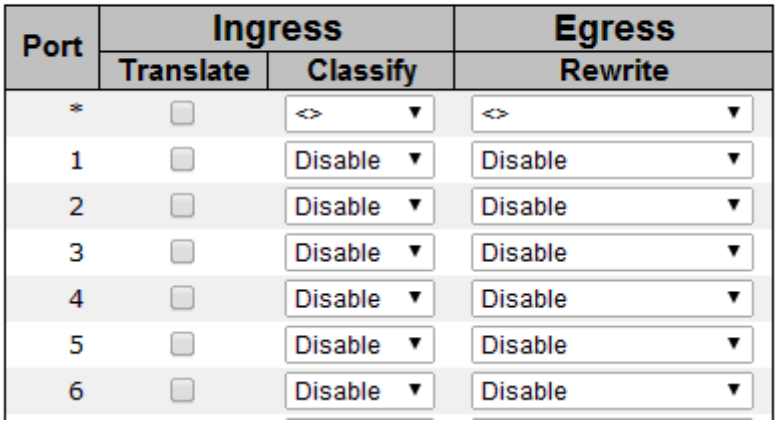
Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified
13	Classified
14	Classified
15	Classified
16	Classified
17	Classified
18	Classified
19	Classified
20	Classified

Label	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking
Mode	Shows the tag remarking mode for this port. Classified: Use classified PCP/DEI values. Default: Use default PCP/DEI values. Mapped: Use mapped versions of QoS class and DP level.

5.1.8.4 Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.

QoS Port DSCP Configuration

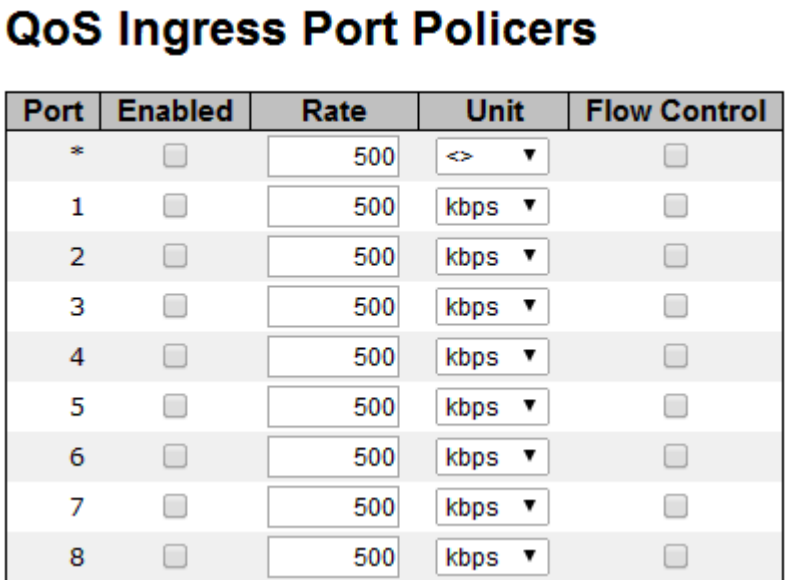


Label	Description
Port	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
Ingress	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: 1. Translate 2. Classify
1. Translate	To Enable the Ingress Translation click the checkbox.
2. Classify	Classification for a port have 4 different values. ・Disable: No Ingress DSCP Classification. ・DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0. ・Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP. ・All: Classify all DSCP.
Egress	Port Egress Rewriting can be one of - ・Disable: No Egress rewrite. ・Enable: Rewrite enabled without remapping. ・Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table.

	• Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

5.1.8.5 Port Policing

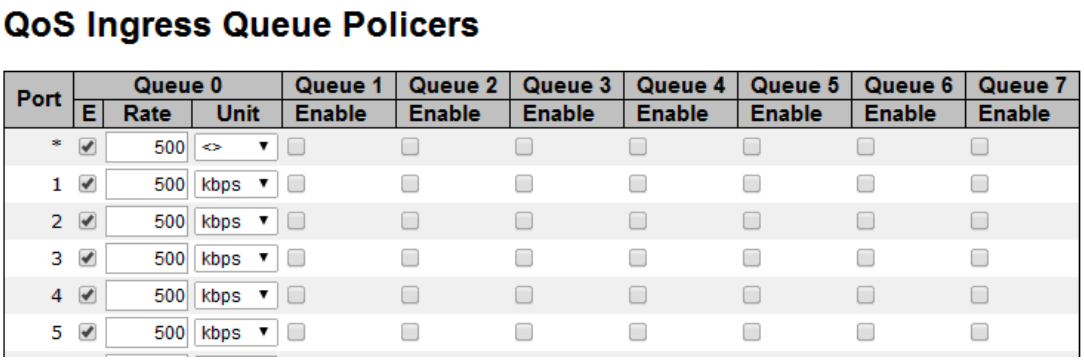
This page allows you to configure the Policer settings for all switch ports.



Label	Description
Port	The port number for which the configuration below applies
Enable	Controls whether the policer is enabled on this switch port.
Rate	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps".
Unti	Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

5.1.8.6 Queue Policing

This page allows you to configure the Queue Policer settings for all switch ports.

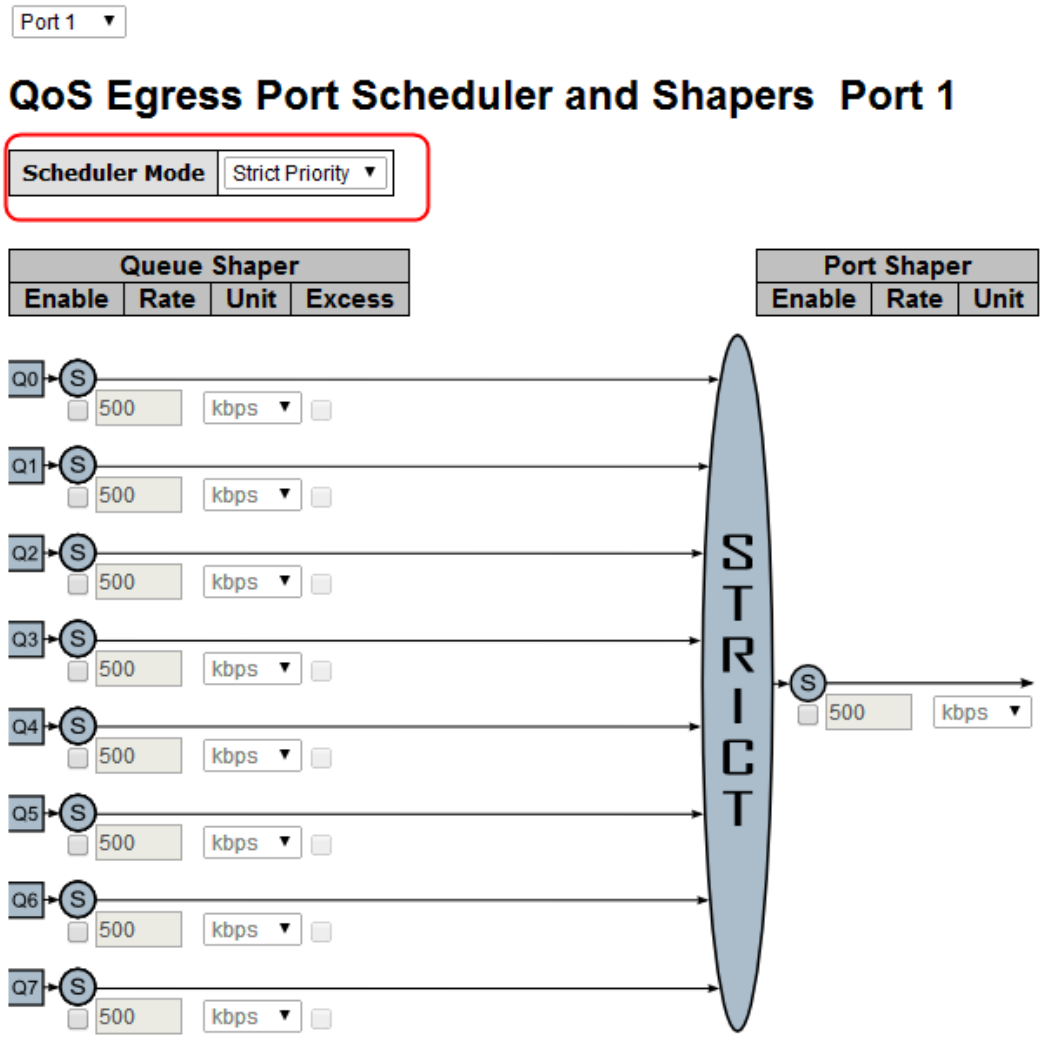


Label	Description
Port	The port number for which the configuration below applies.
Enable(E)	Controls whether the queue policer is enabled on this switch port.
Rate	Controls the rate for the queue policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps". This field is only shown if at least one of the queue policers are enabled.
Unit	Controls the unit of measure for the queue policer rate as kbps or Mbps. The default value is "kbps". This field is only shown if at least one of the queue policers are enabled.

5.1.8.7 QoS Egress Port Scheduler and Shapers

This page allows you to configure the Scheduler and Shapers for a specific port.

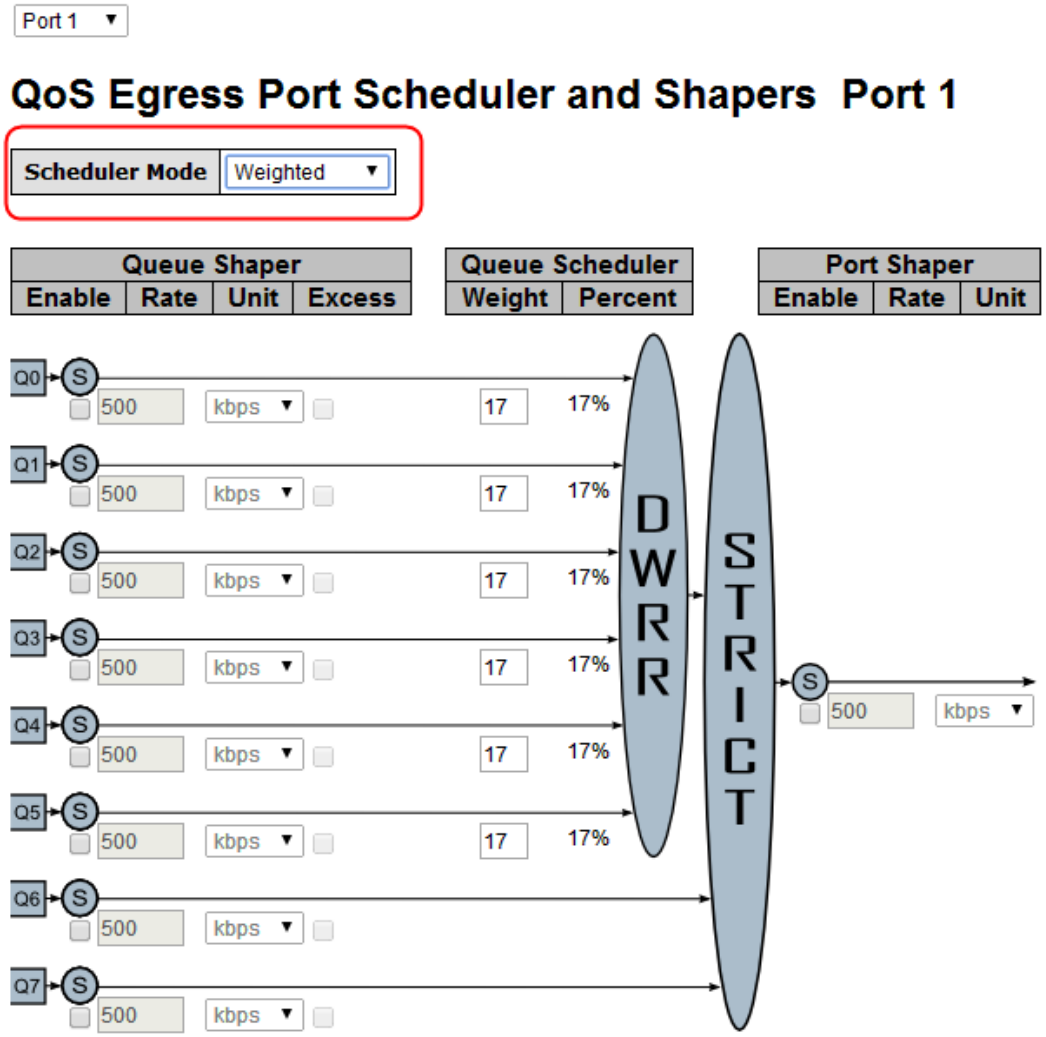
Strict Priority



Label	Description
Scheduler Mode	Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
Queue Shaper Enable	Controls whether the queue shaper is enabled for this queue on this switch port.
Queue Shaper Rate	Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
Queues Shaper Unit	Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
Queue Shaper Excess	Controls whether the queue is allowed to use excess bandwidth.

Port Shaper Enable	Controls whether the port shaper is enabled for this switch port.
Port Shaper Rate	Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
Port Shaper Unit	Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

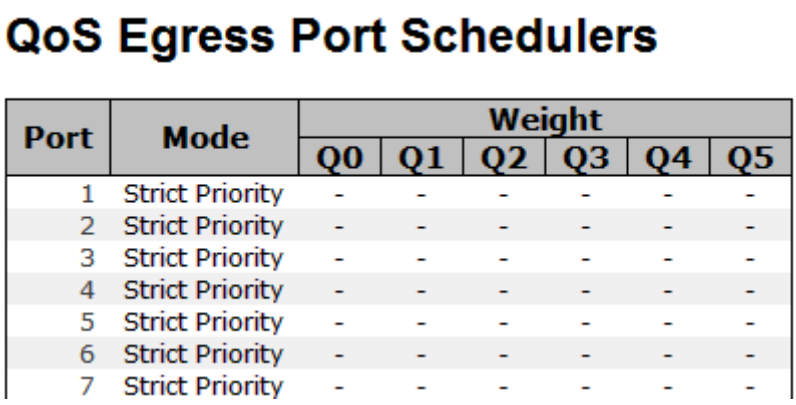
Weighted



Label	Description
Scheduler Mode	Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
Queue Shaper Enable	Controls whether the queue shaper is enabled for this queue on this switch port.
Queue Shaper Rate	Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
Queues Shaper Unit	Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
Queue Shaper Excess	Controls whether the queue is allowed to use excess bandwidth.
Queue Scheduler Weight	Controls the weight for this queue. The default value is "17". This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
Queue Scheduler Percent	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
Port Shaper Enable	Controls whether the port shaper is enabled for this switch port.
Port Shaper Rate	Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps".
Port Shaper Unit	Controls the unit of measure for the port shaper rate as "kbps" or "Mbps". The default value is "kbps".

5.1.8.8 Port Schedulet

This page provides an overview of QoS Egress Port Schedulers for all switch ports.



QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-

Label	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.
Mode	Shows the scheduling mode for this port.
Qn	Shows the weight for this queue and port.

5.1.8.9 Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Label	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.
Mode	Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".
Qn	Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".

5.1.8.10 DSCP Based QoS

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

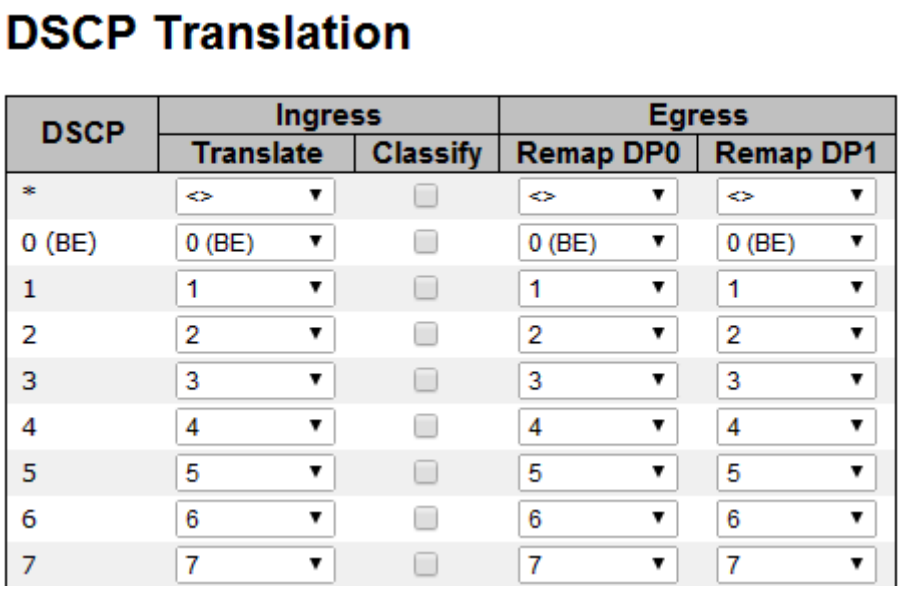
DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	☐	<>	<>
0 (BE)	☐	0	0
1	☐	0	0
2	☐	0	0
3	☐	0	0
4	☐	0	0

Label	Description
DSCP	Maximum number of supported DSCP values are 64..
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
QoS Class	QoS class value can be any of (0-7)
DPL	Drop Precedence Level (0-1)

5.1.8.11 DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

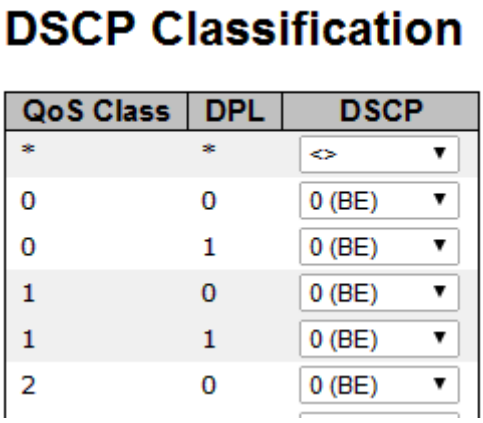


Label	Description
DSCP	Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
Ingress	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation - 1. Translate 2. Classify
1. Translate	DSCP at Ingress side can be translated to any of (0-63) DSCP

	values.
2.Classify	Click to enable Classification at Ingress side.
Egress	There are the following configurable parameters for Egress side – 1. Remap DP0 Controls the remapping for frames with DP level 0. 2. Remap DP1 Controls the remapping for frames with DP level 1.
1.Remap DP0	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.
2.Remap DP1	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

5.1.8.12 DSCP Classification

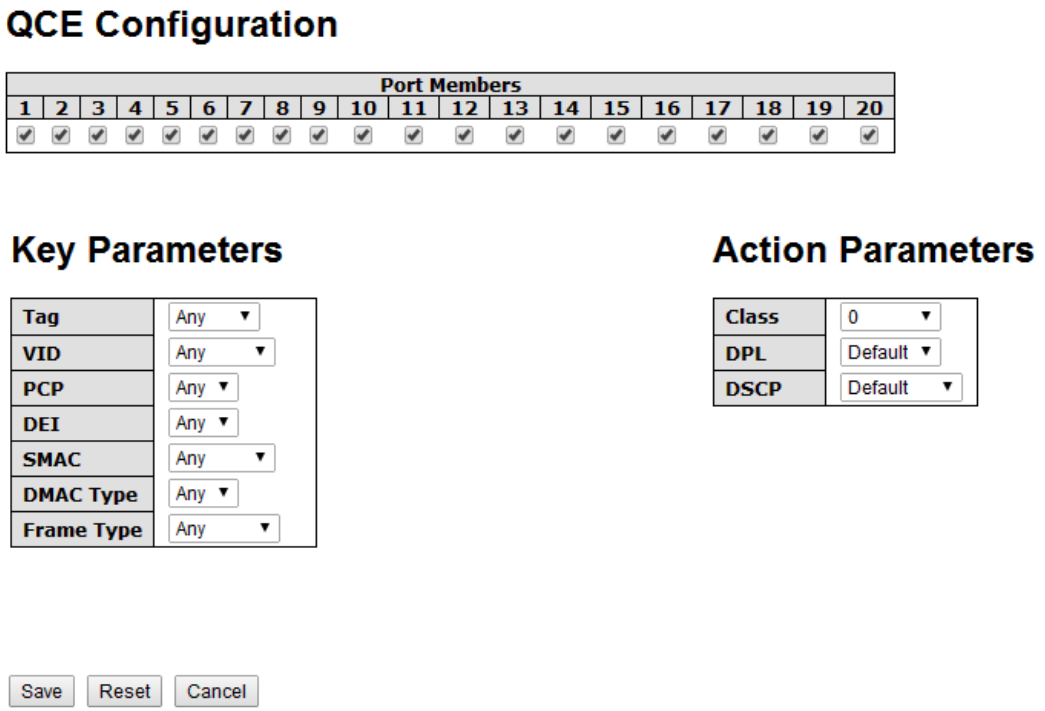
This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.



Label	Description
QoS Class	Actual QoS class
DPL	Actual Drop Precedence Level.
DSCP	Select the classified DSCP value (0-63).

5.1.8.13 QoS Control List

This page allows to edit|insert a single QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the frame type that you select.



Label	Description
Port Members	Check the checkbox button to include the port in the QCL entry. By default all ports are included.
Key Parameters	Key configuration is described as below: Tag Value of Tag field can be 'Any', 'Untag' or 'Tag'. VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs. PCP Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'. DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'. SMAC Source MAC address: 24 MS bits (OUI) or 'Any'. DMAC Type Destination MAC type: possible values are unicast(UC), multicast(MC), broadcast(BC) or 'Any'. Frame Type Frame Type can have any of the following values:

	1. Any 2. Ethernet 3. LLC 4. SNAP 5. IPv4 6. IPv6 Note: All frame types are explained below.
1.Any	Allow all types of frames.
2. Ethernet	Ethernet Type Valid Ethernet type can have a value within 0x600-0xFFFF or 'Any' but excluding 0x800(IPv4) and 0x86DD (IPv6), default value is 'Any'.
3.LLC	SSAP Address Valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'. DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'. Control Valid Control field can vary from 0x00 to 0xFF or 'Any'; the default value is 'Any'.
4.SNAP	PID Valid PID (aka Ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any'.
5.IPv4	Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'. Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. IP Fragment Ipv4 frame fragmented option: yes | no | any. Sport Source TCP/UDP port☹0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP. Dport Destination TCP/UDP port☹0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP
6.IPv6	Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'. Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits. DSCP Diffserv Code Point value (DSCP): It can be a specific

	value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP. Dport Destination TCP/UDP port :(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
Action Parameters	Class QoS class: (0-7) or 'Default'. DP Valid Drop Precedence Level can be (0-1) or 'Default'. DSCP Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'. 'Default' means that the default classified value is not modified by this QCE.

5.1.8.14 QoS Counters

This page provides statistics for the different queues for all switch ports.

Queuing Counters

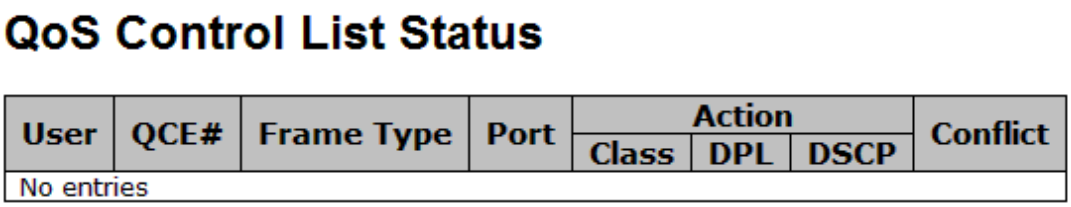
Auto-refresh ☐ Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	4834	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4144
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	16139	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13406
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Label	Description
Port	The logical port for the settings contained in the same row.
Qn	There are 8 QoS queues per port. Q0 is the lowest priority queue.
Rx / Tx	The number of received and transmitted packets per queue.

5.1.8.15 QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.



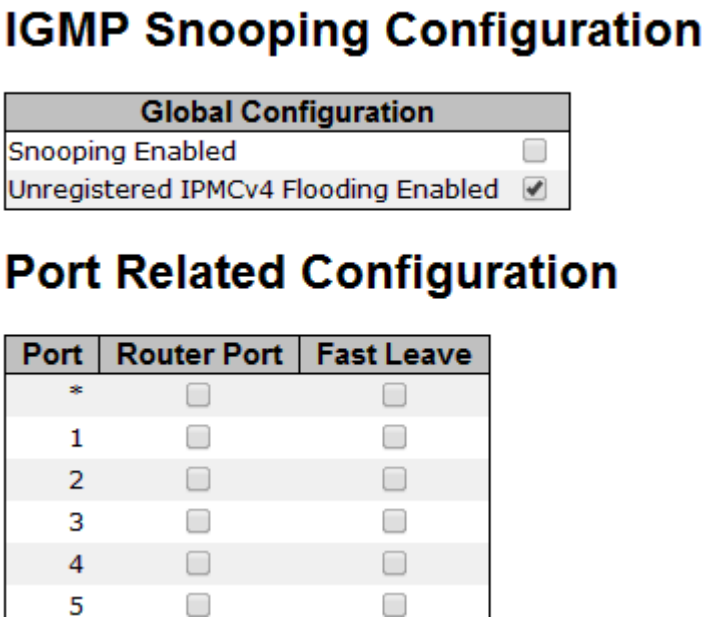
Label	Description
User	Indicates the QCL user.
QCE#	Indicates the index of QCE.
Frame Type	Indicates the type of frame to look for incoming frames. Possible frame types are: Any: The QCE will match all frame type. Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. LLC: Only (LLC) frames are allowed. SNAP: Only (SNAP) frames are allowed. IPv4: The QCE will match only IPV4 frames. IPv6: The QCE will match only IPV6 frames.
Port	Indicates the list of ports configured with the QCE.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP. Class: Classified QoS class; if a frame matches the QCE it will be put in the queue. DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column. DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.
Conflict	Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows

	conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

5.1.9 Multicast

5.1.9.1 IGMP Snooping

This page provides IGMP Snooping related configuration.



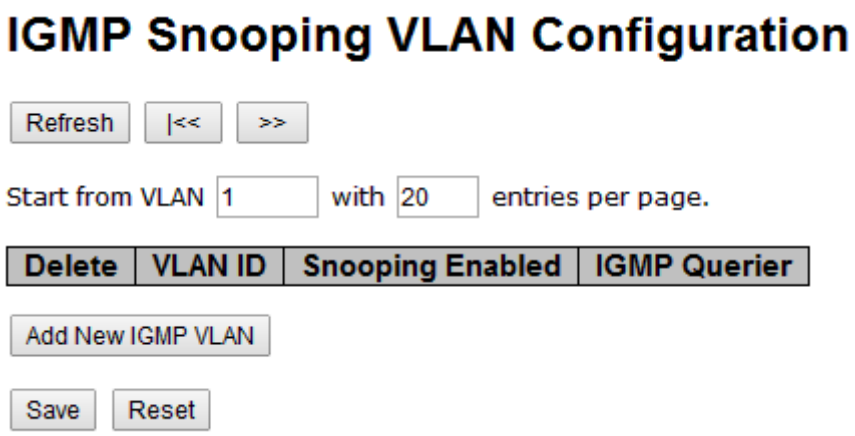
Label	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMCv4Flooding enabled	Enable unregistered IPMC traffic flooding.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port.

5.1.9.2 IGMP Snooping- VLAN Configuration-

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the Refresh button will update the displayed table starting from that or the next closest VLAN Table match.

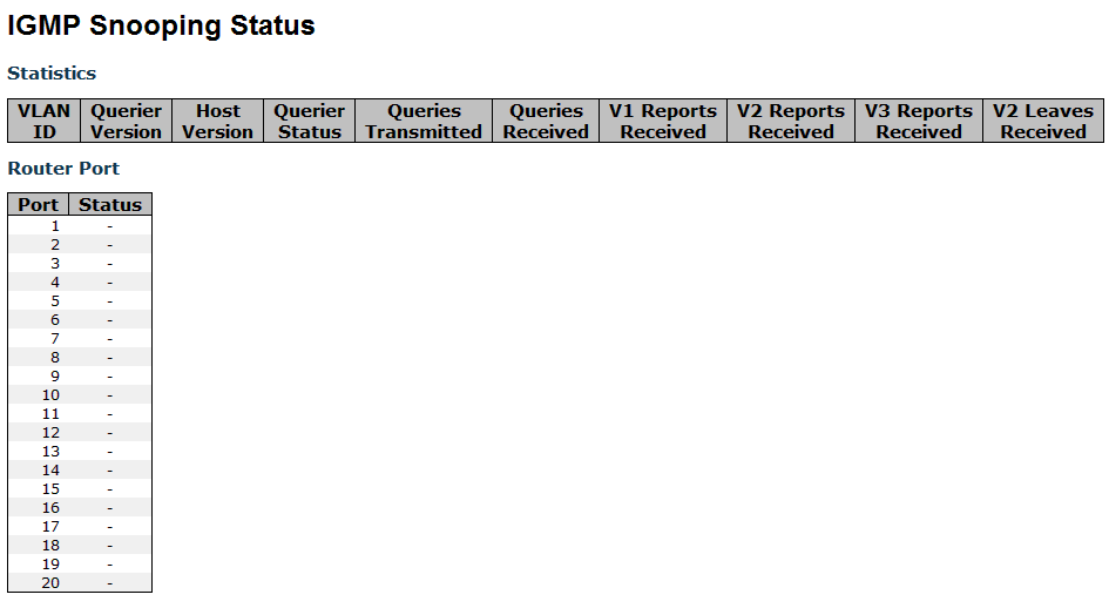
The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.



Label	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enable	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
IGMP Querier	Enable the IGMP Querier in the VLAN.

5.1.9.3 IGMP Snooping Status

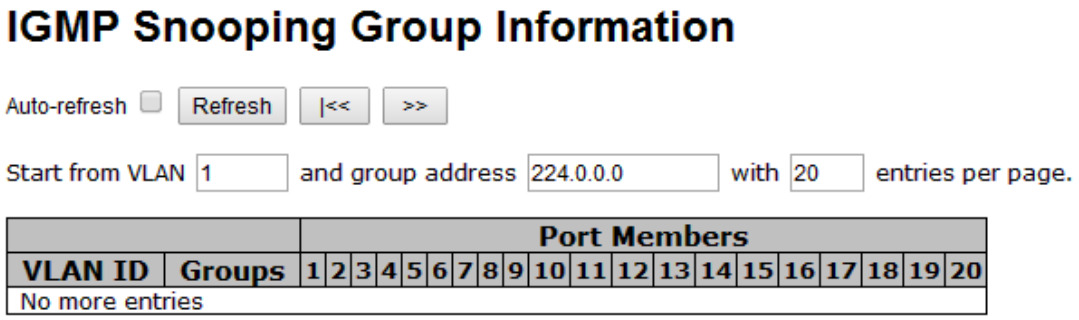
This page provides IGMP Snooping status.


IGMP Snooping Status
Statistics
VLAN ID
Querier Version
Host Version
Querier Status
Queries Transmitted
Queries Received
V1 Reports Received
V2 Reports Received
V3 Reports Received
V2 Leaves Received
Router Port
Port
Status
1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9 - 10 - 11 - 12 - 13 - 14 - 15 - 16 - 17 - 18 - 19 - 20 -

Label	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
Querier Status	Show the Querier status is "ACTIVE" or "IDLE".
Querier Receive	The number of Transmitted Querier.
V1 Reports Receive	The number of Received V1 Reports.
V2 Reports Receive	The number of Received V2 Reports.
V3 Reports Receive	The number of Received V3 Reports.
V2 Leave Receive	The number of Received V2 Leave.
Refresh	Click to refresh the page immediately.
Clear	Clears all Statistics counters.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.
Port	Switch Port number
Status	Indicate whether specific port is a router port or not .

5.1.9.4 IGMP Snooping Groups Information

Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.


IGMP Snooping Group Information
Auto-refresh
Refresh
|<<
>>
Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.
Port Members
VLAN ID Groups 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
No more entries

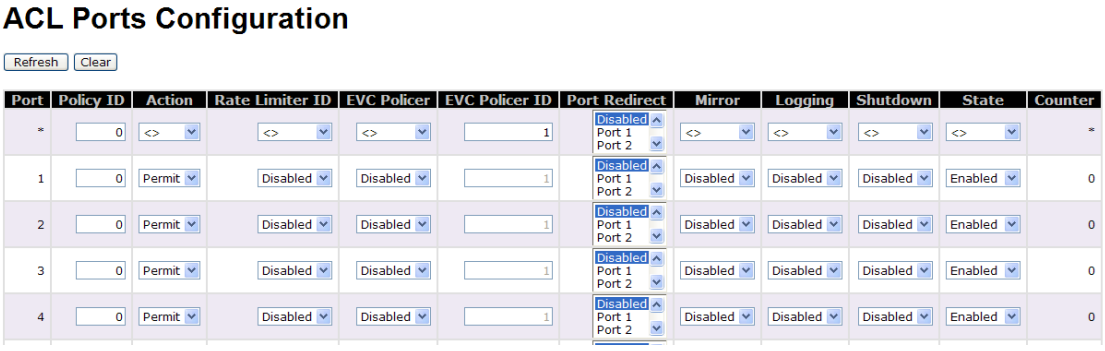
Label	Description
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group..

5.1.10 Security

5.1.10.1 ACL

5.1.10.1.1 Ports

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

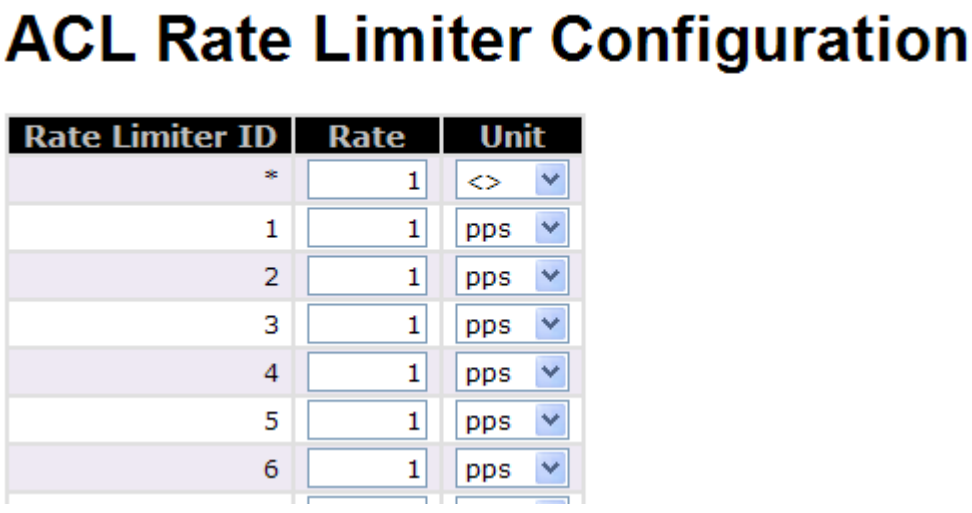


Label	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are 1 through 8. The default value is 1.

Action	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
Rate Limiter ID	Select which rate limiter to apply to this port. The allowed values are Disabled or the values 1 through 15. The default value is "Disabled".
Port Copy	Select which port frames are copied to. The allowed values are Disabled or a specific port number. The default value is "Disabled".
Logging	Specify the logging operation of this port. The allowed values are: Enabled: Frames received on the port are stored in the System Log. Disabled: Frames received on the port are not logged. The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of this port. The allowed values are: Enabled: If a frame is received on the port, the port will be disabled. Disabled: Port shut down is disabled. The default value is "Disabled".
Counter	Counts the number of frames that match this ACE.

5.1.10.1.2 Rate Limiters

Configure the rate limiter for the ACL of the switch.



Label	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The rate unit is packet per second (pps), configure the rate as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K.

	The 1 kpps is actually 1002.1 pps.

5.1.10.1.3 ACL Control List

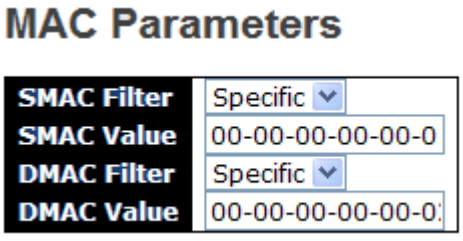
Configure an ACE (Access Control Entry) on this page.

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type that you selected.

A frame that hits this ACE matches the configuration that is defined here.

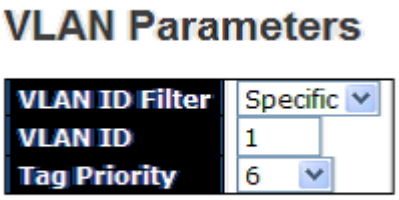
Label	Description
Ingress Port	Select the ingress port for which this ACE applies. Any: The ACE applies to any port. Port n: The ACE applies to this port number, where n is the number of the switch port. Policy n: The ACE applies to this policy number, where n can range from 1 through 8.
Frame Type	Select the frame type for this ACE. These frame types are mutually exclusive. Any: Any frame can match this ACE. Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 descripts the value of Length/Type Field specifications should be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with etnernet type. IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with etnernet type.

Action	Specify the action to take with a frame that hits this ACE. Permit: The frame that hits this ACE is granted permission for the ACE operation. Deny: The frame that hits this ACE is dropped.
Rate Limiter	Specify the rate limiter in number of base units. The allowed range is 1 to 15. Disabled indicates that the rate limiter operation is disabled.
Port Copy	Frames that hit the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port copy operation is disabled.
Logging	Specify the logging operation of the ACE. The allowed values are: Enabled: Frames matching the ACE are stored in the System Log. Disabled: Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of the ACE. The allowed values are: Enabled: If a frame matches the ACE, the ingress port will be disabled. Disabled: Port shut down is disabled for the ACE.
Counter	The counter indicates the number of times the ACE was hit by a frame.

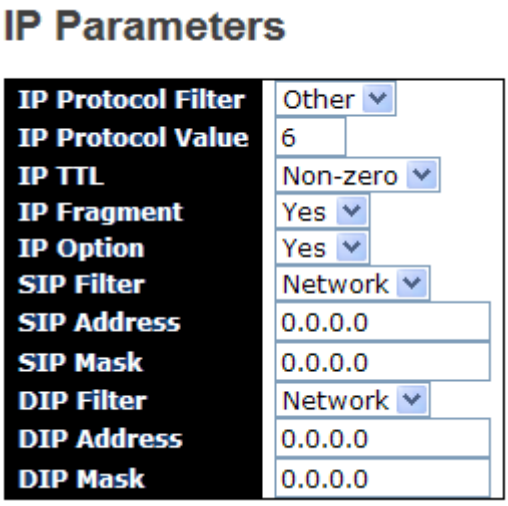


Label	Description
SMAC Filter	(Only displayed when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE. Any: No SMAC filter is specified. (SMAC filter status is "don't-care".) Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

SMAC Value	When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SMAC value.
DMAC Filter	Specify the destination MAC filter for this ACE. Any: No DMAC filter is specified. (DMAC filter status is "don't-care".) MC: Frame must be multicast. BC: Frame must be broadcast. UC: Frame must be unicast. Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.
DMAC Value	When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DMAC value.



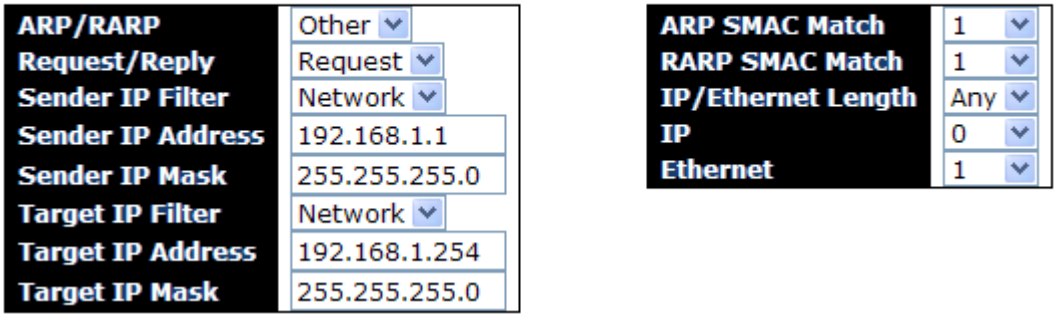
Label	Description
VLAN ID Filter	Specify the VLAN ID filter for this ACE. Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.
VLAN ID	When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.
Tag Priority	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)



Label	Description
IP Protocol Filter	Specify the IP protocol filter for this ACE. Any: No IP protocol filter is specified ("don't-care"). Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears. ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file. UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file. TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.
IP Protocol Value	When "Specific" is selected for the IP protocol value, you can enter a specific value.. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.
IP TTL	Specify the Time-to-Live settings for this ACE. Zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry. Non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry. Any: Any value is allowed ("don't-care").
IP Fragment	Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset

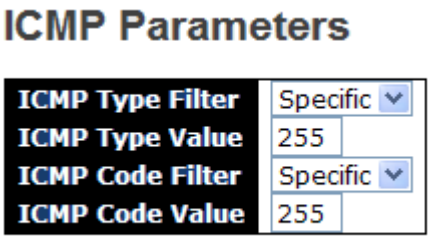
	(FRAG OFFSET) field for an IPv4 frame. No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry. Any: Any value is allowed ("don't-care").
IP Option	Specify the options flag setting for this ACE. No: IPv4 frames where the options flag is set must not be able to match this entry. Yes: IPv4 frames where the options flag is set must be able to match this entry. Any: Any value is allowed ("don't-care").
SIP Filter	Specify the source IP filter for this ACE. Any: No source IP filter is specified. (Source IP filter is "don't-care".) Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears. Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.
SIP Address	When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.
SIP Mask	When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
DIP Filter	Specify the destination IP filter for this ACE. Any: No destination IP filter is specified. (Destination IP filter is "don't-care".) Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears. Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.
DIP Address	When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.
DIP Mask	When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

ARP Parameters

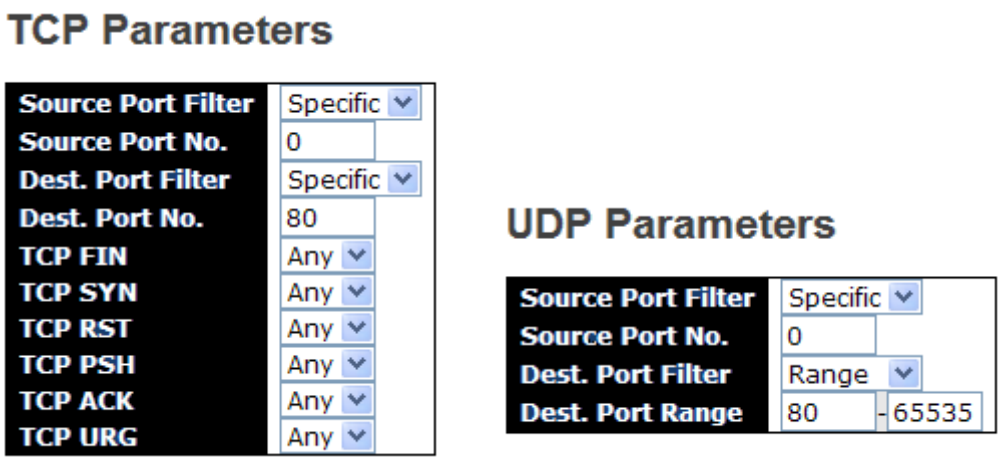


Label	Description
ARP/RARP	Specify the available ARP/RARP opcode (OP) flag for this ACE. Any: No ARP/RARP OP flag is specified. (OP is "don't-care".) ARP: Frame must have ARP/RARP opcode set to ARP. RARP: Frame must have ARP/RARP opcode set to RARP. Other: Frame has unknown ARP/RARP Opcode flag.
Request/Reply	Specify the available ARP/RARP opcode (OP) flag for this ACE. Any: No ARP/RARP OP flag is specified. (OP is "don't-care".) Request: Frame must have ARP Request or RARP Request OP flag set. Reply: Frame must have ARP Reply or RARP Reply OP flag.
Sender IP Filter	Specify the sender IP filter for this ACE. Any: No sender IP filter is specified. (Sender IP filter is "don't-care".) Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears. Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.
Sender IP Address	When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.
Sender IP Mask	When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
Target IP Filter	Specify the target IP filter for this specific ACE. Any: No target IP filter is specified. (Target IP filter is "don't-care".) Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in

	the Target IP Address and Target IP Mask fields that appear.
Target IP Address	When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.
Target IP Mask	When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.
ARP SMAC Match	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. 0: ARP frames where SHA is not equal to the SMAC address. 1: ARP frames where SHA is equal to the SMAC address. Any: Any value is allowed ("don't-care").
RARP SMAC Match	Specify whether frames can hit the action according to their target hardware address field (THA) settings. 0: RARP frames where THA is not equal to the SMAC address. 1: RARP frames where THA is equal to the SMAC address. Any: Any value is allowed ("don't-care").
IP/Ethernet Length	Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings. 0: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must not match this entry. 1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must match this entry. Any: Any value is allowed ("don't-care").
IP	Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings. 0: ARP/RARP frames where the HLD is equal to Ethernet (1) must not match this entry. 1: ARP/RARP frames where the HLD is equal to Ethernet (1) must match this entry. Any: Any value is allowed ("don't-care").
Ethernet	Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings. 0: ARP/RARP frames where the PRO is equal to IP (0x800) must not match this entry. 1: ARP/RARP frames where the PRO is equal to IP (0x800) must match this entry. Any: Any value is allowed ("don't-care").



Label	Description
ICMP Type Filter	Specify the ICMP filter for this ACE. Any: No ICMP filter is specified (ICMP filter status is "don't-care"). Specific: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.
ICMP Type Value	When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.
ICMP Code Filter	Specify the ICMP code filter for this ACE. Any: No ICMP code filter is specified (ICMP code filter status is "don't-care"). Specific: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.
ICMP Code Value	When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.



Label	Description
TCP/UDP Source Filter	Specify the TCP/UDP source filter for this ACE. Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care"). Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears. Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.
TCP/UDP Source No.	When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.
TCP/UDP Source Range	When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.
TCP/UDP Destination Filter	Specify the TCP/UDP destination filter for this ACE. Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care"). Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears. Range: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination

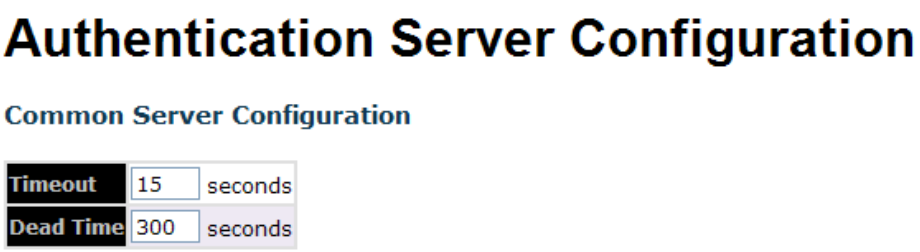
	range value. A field for entering a TCP/UDP destination value appears.
TCP/UDP Destination Number	When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.
TCP/UDP Destination Range	When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.
TCP FIN	Specify the TCP "No more data from sender" (FIN) value for this ACE. 0: TCP frames where the FIN field is set must not be able to match this entry. 1: TCP frames where the FIN field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP SYN	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. 0: TCP frames where the SYN field is set must not be able to match this entry. 1: TCP frames where the SYN field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP PSH	Specify the TCP "Push Function" (PSH) value for this ACE. 0: TCP frames where the PSH field is set must not be able to match this entry. 1: TCP frames where the PSH field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP ACK	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. 0: TCP frames where the ACK field is set must not be able to match this entry. 1: TCP frames where the ACK field is set must be able to match this entry. Any: Any value is allowed ("don't-care").

TCP URG	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. 0: TCP frames where the URG field is set must not be able to match this entry. 1: TCP frames where the URG field is set must be able to match this entry. Any: Any value is allowed ("don't-care").

5.1.10.2 AAA

5.1.10.2.1 Common Server Configuration

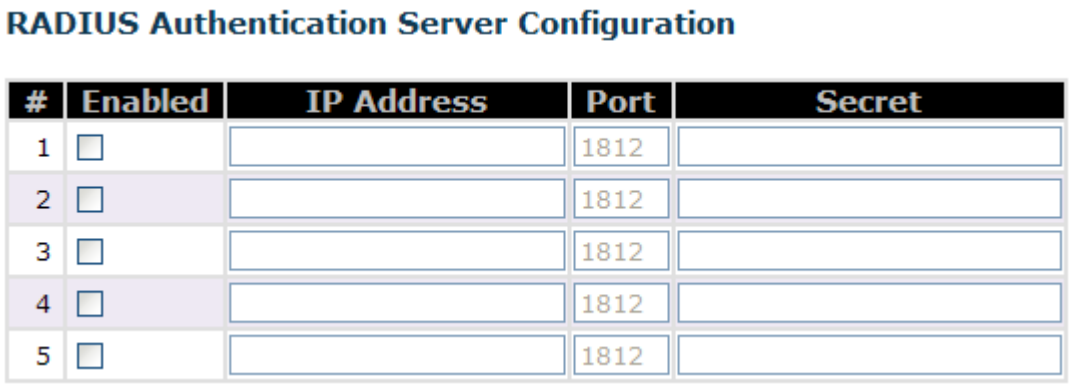
This page allows you to configure the Authentication Servers



Label	Description
Timeout	The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this time frame, we will consider it to be dead and continue with the next enabled server (if any). RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.
Dead Time	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

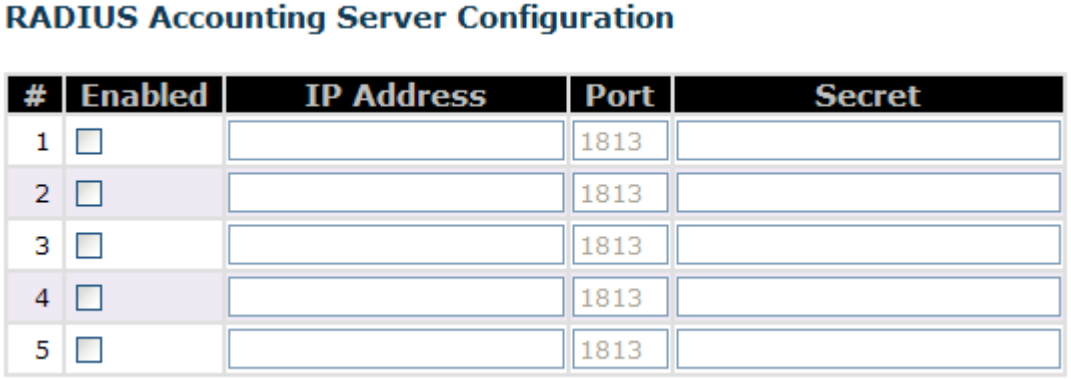
5.1.10.2.2 RADIUS Authentication Server Configuration

The table has one row for each RADIUS Authentication Server and a number of columns, which are:



Label	Description
#	The RADIUS Authentication Server number for which the configuration below applies.
Enabled	Enable the RADIUS Authentication Server by checking this box.
IP Address	The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.
Port	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.
Secret	The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the switch stack.

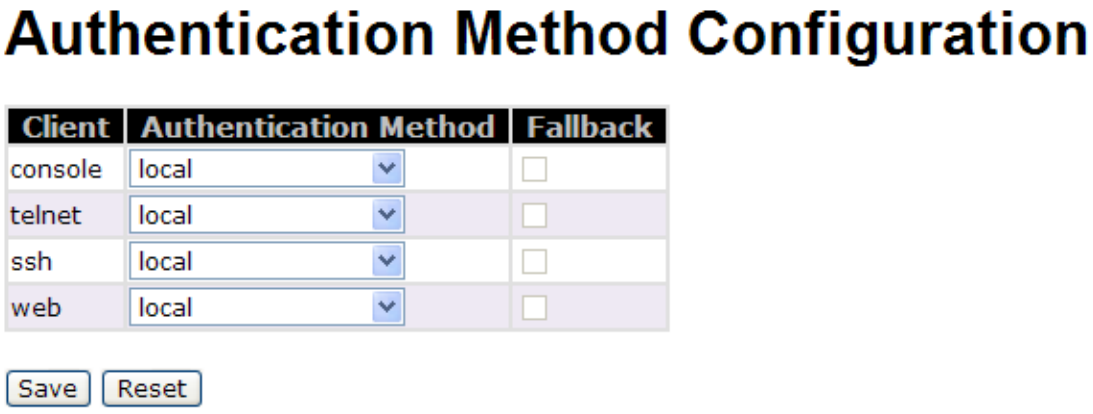
5.1.10.2.3 RADIUS Accounting Server Configuration



Label	Description
#	The RADIUS Accounting Server number for which the configuration below applies.
Enabled	Enable the RADIUS Accounting Server by checking this box.
IP Address	The IP address or hostname of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.
Port	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
Secret	The secret - up to 29 characters long - shared between the RADIUS Accounting Server and the switch stack.

5.1.10.3 Auth Method

This page allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.



Label	Description
Client	The management client for which the configuration below applies.
Authentication Mothod	Authentication Method can be set to one of the following values: none: authentication is disabled and login is not possible. local: use the local user database on the switch for authentication. radius: use a remote RADIUS server for authentication.
Fallback	Enable fallback to local authentication by checking this box. If none of the configured authentication servers are alive, the local user database is used for authentication.

	This is only possible if the Authentication Method is set to a value other than 'none' or 'local'.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.10.4 RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.

RADIUS Authentication Servers

RADIUS Authentication Server Status Overview

Auto-refresh ☐ Refresh

#	IP Address	Status
1	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
Status	The current status of the server. This field takes one of the following values: Disabled: The server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more

	than one server is enabled.

RADIUS Accounting Servers

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
Status	The current status of the server. This field takes one of the following values: Disabled: The server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

5.1.10.5 RADIUS Details

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Use the server select box to switch between the backend servers to show details for.

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

Use the server select box to switch between the backend servers to show details for.

RADIUS Authentication Statistics for Server #1

Server #1 Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		

Other Info	
IP Address	0.0.0.0:1812
State	Disabled
Round-Trip Time	0 ms

Label	Description
Packet Counters	RADIUS authentication server packet counter. There are seven receiving and four transmit counters.
Other Info	This section contains information about the state of the server and the latest round-trip time.

Direction	Name	RFC4668 Name	Description
Rx	**Access Accepts**	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	**Access Rejects**	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	**Access Challenges**	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	**Malformed Access Responses**	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Rx	**Bad Authenticators**	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	**Unknown Types**	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Rx	**Packets Dropped**	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	**Access Requests**	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	**Access Retransmissions**	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	**Pending Requests**	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx	**Timeouts**	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Name	RFC4668 Name	Description
State	-	Shows the state of the server. It takes one of the following values: `Disabled` : The selected server is disabled. `Not Ready` : The server is enabled, but IP communication is not yet up and running. `Ready` : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. `Dead (X seconds left)` : Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address	0.0.0.0:1813		
State	Disabled		
Round-Trip Time	0 ms		

<table>
<tr><th>Label</th><th>Description</th></tr>
<tr><td>Packet Counters</td><td>RADIUS accounting server packet counter. There are five receive and four transmit counters.
<table>
<tr><th>Direction</th><th>Name</th><th>RFC4670 Name</th><th>Description</th></tr>
<tr><td>Rx</td><td>Responses</td><td>radiusAccClientExtResponses</td><td>The number of RADIUS packets (valid or invalid) received from the server.</td></tr>
<tr><td>Rx</td><td>Malformed Responses</td><td>radiusAccClientExtMalformedResponses</td><td>The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or or unknown types are not included as malformed access responses.</td></tr>
<tr><td>Rx</td><td>Bad Authenticators</td><td>radiusAcctClientExtBadAuthenticators</td><td>The number of RADIUS packets containing invalid authenticators received from the server.</td></tr>
<tr><td>Rx</td><td>Unknown Types</td><td>radiusAccClientExtUnknownTypes</td><td>The number of RADIUS packets of unknown types that were received from the server on the accounting port.</td></tr>
<tr><td>Rx</td><td>Packets Dropped</td><td>radiusAccClientExtPacketsDropped</td><td>The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.</td></tr>
<tr><td>Tx</td><td>Requests</td><td>radiusAccClientExtRequests</td><td>The number of RADIUS packets sent to the server. This does not include retransmissions.</td></tr>
<tr><td>Tx</td><td>Retransmissions</td><td>radiusAccClientExtRetransmissions</td><td>The number of RADIUS packets retransmitted to the RADIUS accounting server.</td></tr>
<tr><td>Tx</td><td>Pending Requests</td><td>radiusAccClientExtPendingRequests</td><td>The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.</td></tr>
<tr><td>Tx</td><td>Timeouts</td><td>radiusAccClientExtTimeouts</td><td>The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.</td></tr>
</table></td></tr>
<tr><td>Other Info</td><td>This section contains information about the state of the server and the latest
<table>
<tr><th>Name</th><th>RFC4670 Name</th><th>Description</th></tr>
<tr><td>State</td><td>-</td><td>Shows the state of the server. It takes one of the following values:
<code>Disabled</code> : The selected server is disabled.
<code>Not Ready</code> : The server is enabled, but IP communication is not yet up and running.
<code>Ready</code> : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.
<code>Dead (X seconds left)</code> : Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</td></tr>
<tr><td>Round-Trip Time</td><td>radiusAccClientExtRoundTripTime</td><td>The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.</td></tr>
</table></td></tr>
</table>

5.1.10.6 NAS(802.1x)

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the Authentication configuration page.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1 X authentications.

Overview of 802.1X (Port-Based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server is RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the Authentication configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch

will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Overview of MAC-Based Authentication

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

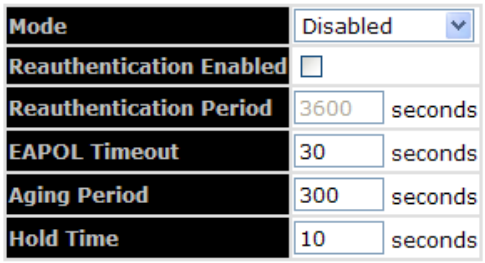
When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.

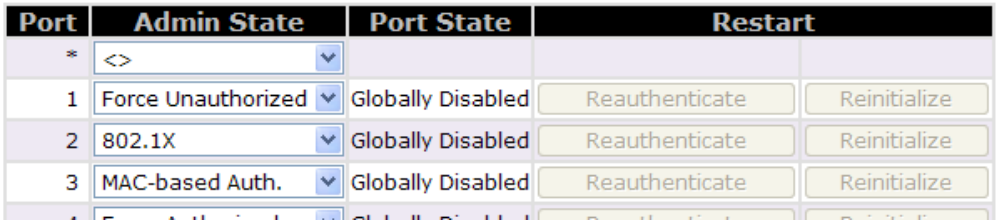
The 802.1X and MAC-Based Authentication configuration consists of two sections, a system- and a port-wide

Network Access Server Configuration

System Configuration



Port Configuration



Label	Description
Mode	Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
Re-authentication Enabled	If checked, clients are re-authenticated after the interval specified by the Re-authentication Period. Re-authentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port. For MAC-based ports, re-authentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Age Period below).
Re-authentication Period	Determines the period, in seconds, after which a connected client must be re-authenticated. This is only active if the Re-authentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
EAPOL Timeout	Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no

	effect for MAC-based ports.
Age Period	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • MAC-Based Auth. When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. For ports in MAC-based Auth. mode, re-authentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.
Hold Time	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • MAC-Based Auth. If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration → Security → AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. The switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.
Port	The port number for which the configuration below applies.
Admin State	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: **Force Authorized** In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication. **Force Unauthorized** In this mode, the switch will send one EAPOL Failure frame when

	the port link comes up, and any client on the port will be disallowed network access. **Port-based 802.1X** In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch is special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant. Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next

	backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate. Single 802.1X In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated. Multi 802.1X In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant. Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or

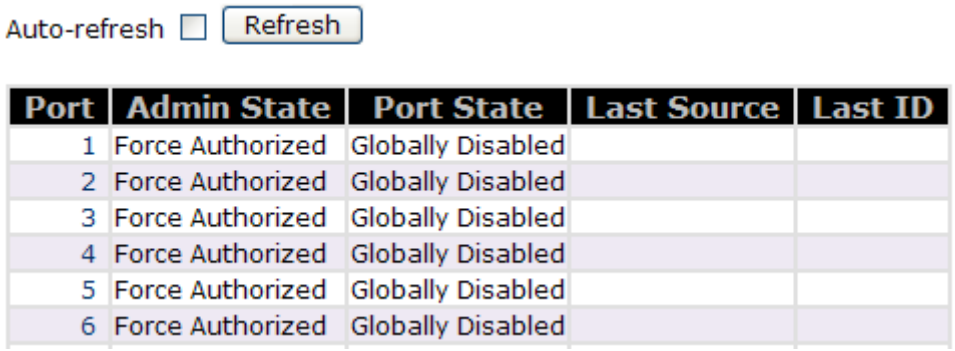
	more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module. In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality. **MAC-based Auth.** Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

	The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.
Port State	The current state of the port. It can undertake one of the following values: **Globally Disabled**: NAS is globally disabled. **Link Down**: NAS is globally enabled, but there is no link on the port. **Authorized**: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. **Unauthorized:** The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. **X Auth/Y Unauth**: The port is in a multi-supplicant mode. Currently X clients are authorized and Y is unauthorized.
Restart	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect. **Re-authenticate**: Schedules a re-authentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, re-authentication will be attempted immediately. The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

	Reinitialize: Forces a re-initialization of the clients on the port and thereby a re-authentication immediately. The clients will transfer to the unauthorized state while the re-authentication is in progress.

Switch

This page provides an overview of the current NAS port states.



Label	Description
Port	The switch port number. Click to navigate to detailed 802.1X statistics for this port.
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
Last Source	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

This page provides detailed IEEE 802.1X statistics for a specific switch port running port-based authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only. Use the port select box to select which port details to be displayed.

Label	Description
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
EAPOL Counters	These supplicant frame counters are available for the following administrative states: • Force Authorized • Force Unauthorized • 802.1X
Backend Server Counters	These backend (RADIUS) frame counters are available for the following administrative states: • 802.1X • MAC-based Auth.

EAPOL Counters

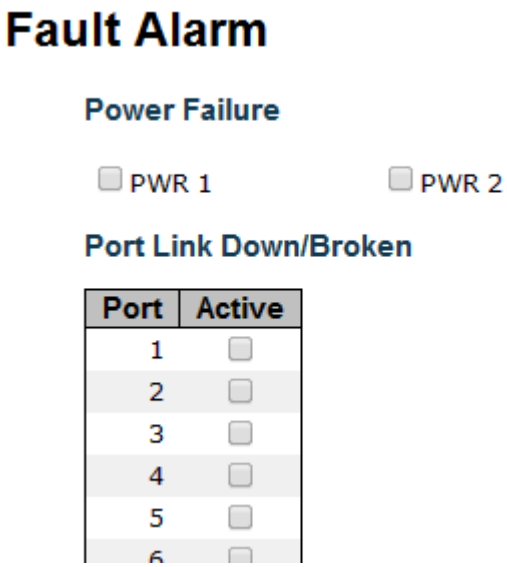
Direction	Name	IEEE Name	Description
Rx	**Total**	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	**Response ID**	dot1xAuthEapolRespIdFramesRx	The number of valid EAP Resp/ID frames that have been received by the switch.
Rx	**Responses**	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.
Rx	**Start**	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	**Logoff**	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL logoff frames that have been received by the switch.
Rx	**Invalid Type**	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	**Invalid Length**	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	**Total**	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	**Request ID**	dot1xAuthEapolReqIdFramesTx	The number of EAP initial request frames that have been transmitted by the switch.
Tx	**Requests**	dot1xAuthEapolReqFramesTx	The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch.

	Backend Server Counters **Direction** | **Name** | **IEEE Name** | **Description** Rx | **Access Challenges** | dot1xAuthBackendAccessChallenges | **Port-based**: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. **MAC-based**: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table). Rx | **Other Requests** | dot1xAuthBackendOtherRequestsToSupplicant | **Port-based**: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. **MAC-based**: Not applicable. Rx | **Auth. Successes** | dot1xAuthBackendAuthSuccesses | **Port- and MAC-based**: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server. Rx | **Auth. Failures** | dot1xAuthBackendAuthFails | **Port- and MAC-based**: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server. Tx | **Responses** | dot1xAuthBackendResponses | **Port-based:** Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. **MAC-based:** Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.
Last Supplicant/Client Info	Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states: • 802.1X • MAC-based Auth. **Last Supplicant/Client Info** **Name** | **IEEE Name** | **Description** **MAC Address** | dot1xAuthLastEapolFrameSource | The MAC address of the last supplicant/client. **VLAN ID** | - | The VLAN ID on which the last frame from the last supplicant/client was received. **Version** | dot1xAuthLastEapolFrameVersion | **802.1X-based**: The protocol version number carried in the most recently received EAPOL frame. **MAC-based**: Not applicable. **Identity** | - | **802.1X-based**: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. **MAC-based**: Not applicable.

5.1.11 Warning

5.1.11.1 Fault Alarm

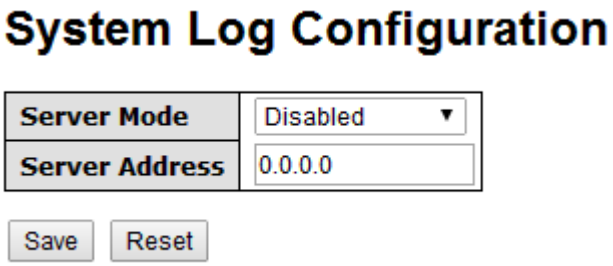
When any selected fault event is happened, the Fault LED in switch panel will light up and the electric relay will signal at the same time.



5.1.11.2 System Warning

5.1.11.2.1 SYSLOG Setting

The SYSLOG is a protocol to transmit event notification messages across networks. Please refer to RFC 3164 - The BSD SYSLOG Protocol



System Warning – SYSLOG Setting interface

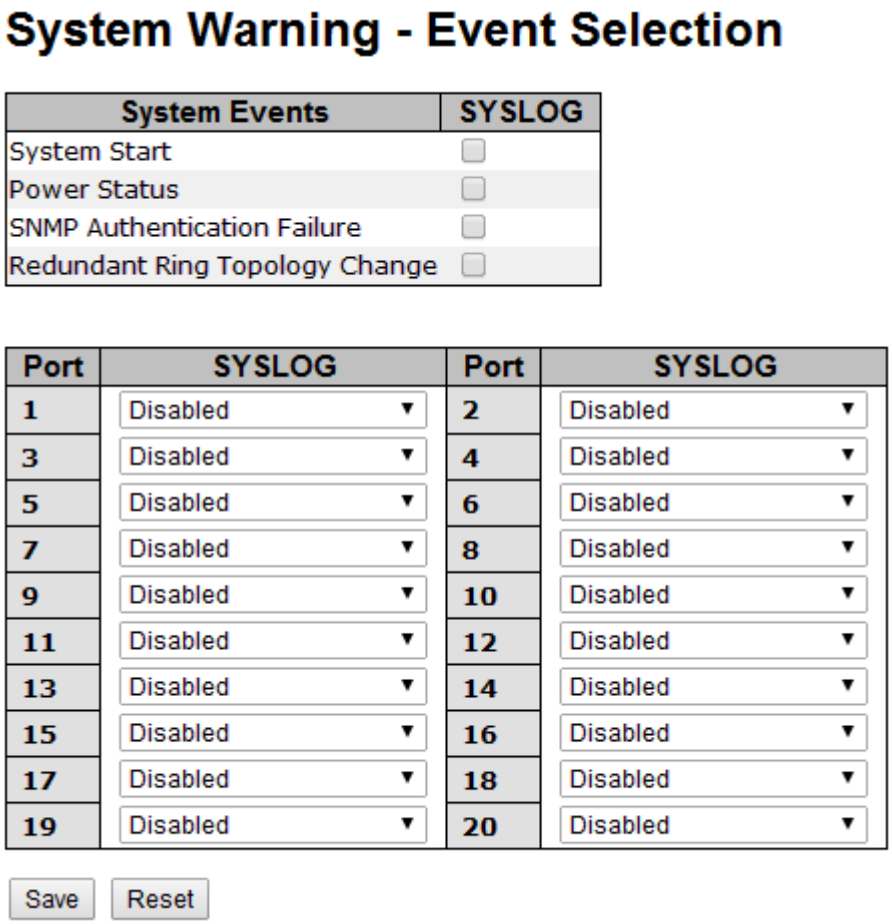
The following table describes the labels in this screen.

Label	Description
Server Mode	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the

	syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are: Enabled: Enable server mode operation. Disabled: Disable server mode operation.
SYSLOG Server IP Address	Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.

5.1.11.2.2 Event Selection

SYSLOG and SMTP are the two warning methods that supported by the system. Check the corresponding box to enable system event warning method you wish to choose. Please note that the checkbox cannot be checked when SYSLOG or SMTP is disabled.



System Warning – Event Selection interface

The following table describes the labels in this screen.

Label	Description
System Cold Start	Alert when system restart
Power Status	Alert when a power up or down
SNMP Authentication Failure	Alert when SNMP authentication failure.
O-Ring Topology Change	Alert when Ring topology changes.
Port Event SYSLOG / SMTP event	■ **Disable** ■ **Link Up** ■ **Link Down** ■ **Link Up & Link Down**
Apply	Click "**Apply**" to activate the configurations.
Help	Show help file.

5.1.12 Monitor and Diag

5.1.12.1 MAC Table

5.1.12.1.1 Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

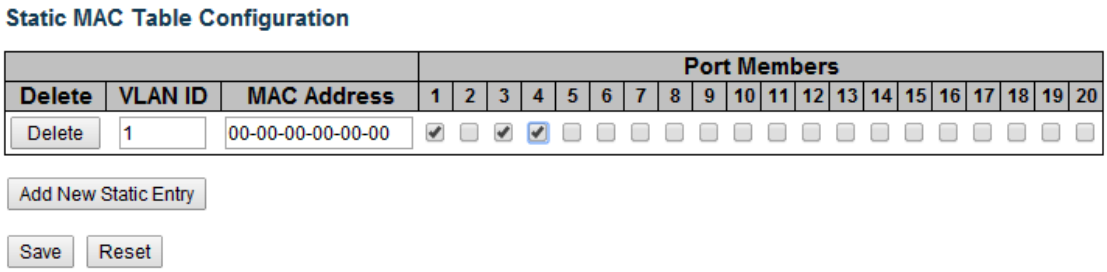
MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	☐
Aging Time	300 seconds

MAC Table Learning

	Port Members																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Auto	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○



Aging Configuration

By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, **Age time** seconds.

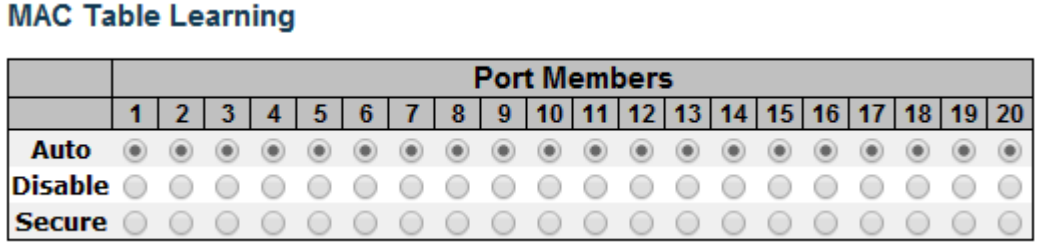
The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking **Disable automatic aging**.

MAC Table Learning

If the learning mode for a given port is grayed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

Each port can do learning based upon the following settings:



Label	Description
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped. Note: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning

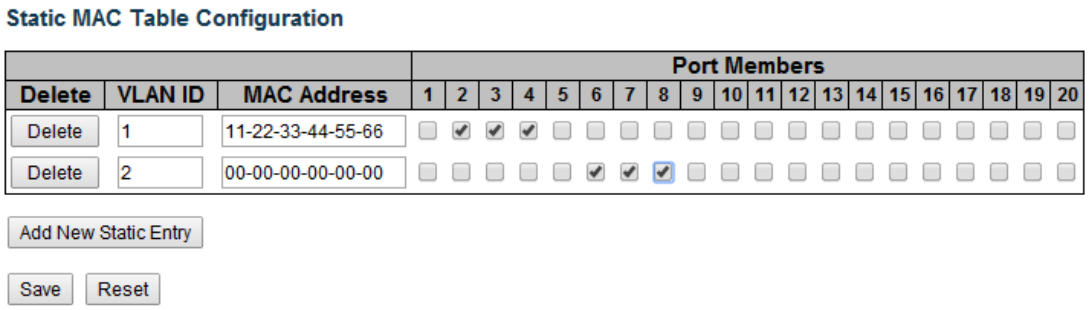
	mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The maximum of 64 entries is for the whole stack, and not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New Static Entry	Click Add new static entry to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

5.1.12.1.2 MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "Start from MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will -

upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "no more entries" is shown in the displayed table. Use the |<< button to start over.

MAC Address Table

Auto-refresh Refresh Clear |<< >>

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

			Port Members																			
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Dynamic	1	00-0E-2E-76-BB-D0							✓														
Static	1	00-1E-94-00-00-00	✓																				
Dynamic	1	00-1E-94-57-81-03							✓														
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Label	Description
Type	Indicates whether the entry is a static or dynamic entry.
MAC address	The MAC address of the entry.
VLAN	The VLAN ID of the entry.
Port Members	The ports that are members of the entry.

5.1.12.2 Port Statistic

5.1.12.2.1 Traffic Overview

This page provides an overview of general traffic statistics for all switch ports.

Port Statistics Overview

Auto-refresh Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	7993	7035	1264795	3640550	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	16139	13406	2391306	5440765	0	0	0	0	3
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0

Label	Description
Port	The logical port for the settings contained in the same row.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Updates the counters entries, starting from the current entry ID.
Clear	Flushes all counters entries.

5.1.12.2.2 Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Detailed Statistics-Receive & Transmit Total

Detailed Port Statistics Port 1

Port 1 ▾ Auto-refresh ☐ Refresh Clear

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Label	Description
Rx and Tx Packets	The number of received and transmitted (good and bad) packets.
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short 1 frames received with valid CRC.
Rx Oversize	The number of long 2 frames received with valid CRC.
Rx Fragments	The number of short 1 frames received with invalid CRC.
Rx Jabber	The number of long 2 frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.
Tx Drops	The number of frames dropped due to output buffer congestion.
Tx Late / Exc.Coll.	The number of frames dropped due to excessive or late collisions.

Short frames are frames that are smaller than 64 bytes.

Long frames are frames that are longer than the configured maximum frame length for this port.

5.1.12.3 Port Mirroring

Configure port Mirroring on this page.

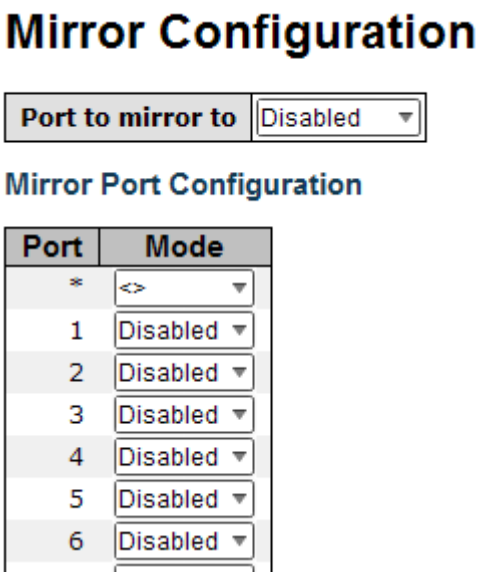
To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.

The traffic to be copied to the mirror port is selected as follows:

All frames received on a given port (also known as ingress or source mirroring).

All frames transmitted on a given port (also known as egress or destination mirroring).

Port mirroring feature – how to configure. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port. Disabled disables mirroring.



Label	Description
Port	The logical port for the settings contained in the same row.
Mode	Select mirror mode. Rx only: Frames received at this port are mirrored to the mirror port. Frames transmitted are not mirrored. Tx only: Frames transmitted from this port are mirrored to the mirror port. Frames received are not mirrored. Disabled: Neither frames transmitted nor frames received are mirrored. Enabled: Frames received and frames transmitted are mirrored to the mirror port. Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames for the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

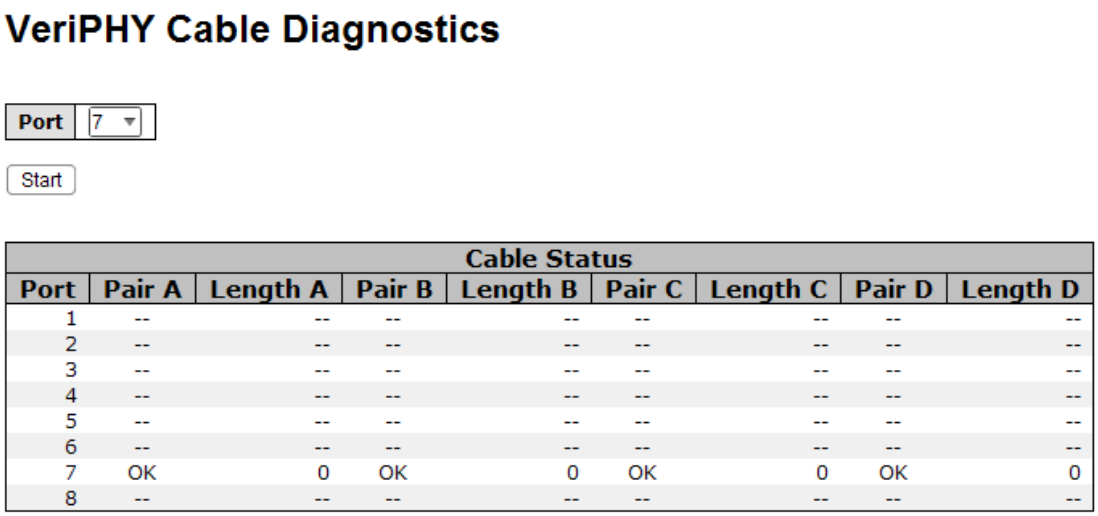
5.1.12.4 System Log Information

The switch system log information is provided here.

Label	Description
ID	The ID (>= 1) of the system log entry.
Level	The level of the system log entry. The following level types are supported: Info: Information level of the system log. Warning: Warning level of the system log. Error: Error level of the system log. All: All levels.
Time	The time of the system log entry.
Message	The MAC Address of this switch.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Updates the system log entries, starting from the current entry ID.
Clear	Flushes all system log entries.
|<<	Updates the system log entries, starting from the first available entry ID.
<<	Updates the system log entries, ending at the last entry currently displayed.
>>	Updates the system log entries, starting from the last entry currently displayed.
>>|	Updates the system log entries, ending at the last available entry ID.

5.1.12.5 Cable Diagnostics

This page is used for running the VeriPHY Cable Diagnostics.

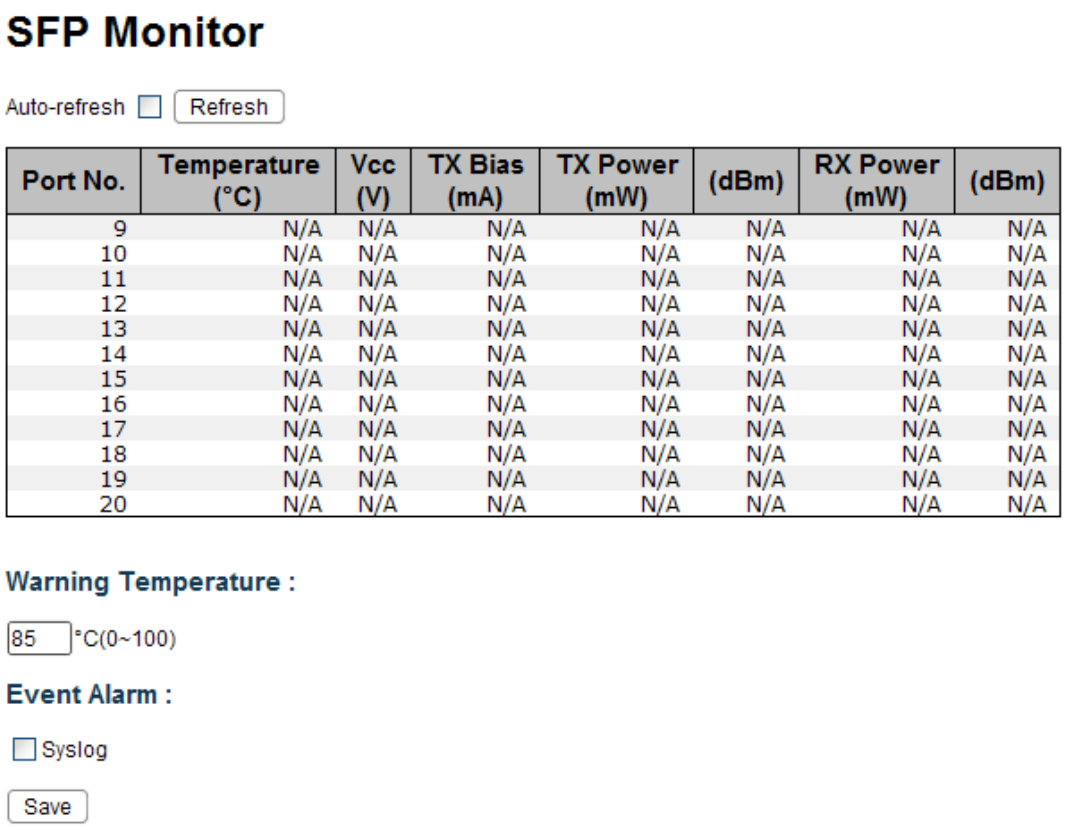

VeriPHY Cable Diagnostics
Port
7
Start
Cable Status
Port Pair A Length A Pair B Length B Pair C Length C Pair D Length D
1 -- -- -- -- -- -- -- -- -- --
2 -- -- -- -- -- -- -- -- -- --
3 -- -- -- -- -- -- -- -- -- --
4 -- -- -- -- -- -- -- -- -- --
5 -- -- -- -- -- -- -- -- -- --
6 -- -- -- -- -- -- -- -- -- --
7 OK 0 OK 0 OK 0 OK 0
8 -- -- -- -- -- -- -- -- -- --

Press Start to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters. 10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Label	Description
Port	The port where you are requesting VeriPHY Cable Diagnostics.
Cable Status	Port: Port number. Pair: The status of the cable pair. Length: The length (in meters) of the cable pair.

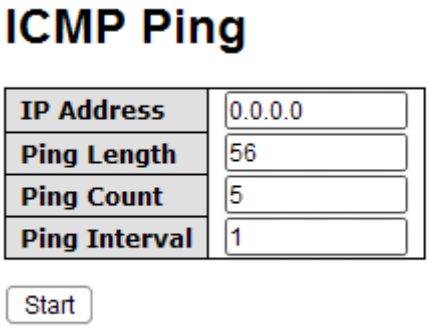
5.1.12.6 SFP Monitor

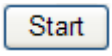
DDM functionality can support SFP modules which support the DDM function. It measure the temperature of the apparatus .You may manage and set up event alarm module through DDM WEB


SFP Monitor
Auto-refresh
Refresh
Port No. Temperature (°C) Vcc (V) TX Bias (mA) TX Power (mW) (dBm) RX Power (mW) (dBm)
9 N/A N/A N/A N/A N/A N/A N/A
10 N/A N/A N/A N/A N/A N/A N/A
11 N/A N/A N/A N/A N/A N/A N/A
12 N/A N/A N/A N/A N/A N/A N/A
13 N/A N/A N/A N/A N/A N/A N/A
14 N/A N/A N/A N/A N/A N/A N/A
15 N/A N/A N/A N/A N/A N/A N/A
16 N/A N/A N/A N/A N/A N/A N/A
17 N/A N/A N/A N/A N/A N/A N/A
18 N/A N/A N/A N/A N/A N/A N/A
19 N/A N/A N/A N/A N/A N/A N/A
20 N/A N/A N/A N/A N/A N/A N/A
Warning Temperature :
85 °C(0~100)
Event Alarm :
Syslog
Save

5.1.12.7 Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.



After you press 

, 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes

automatically until responses to all packets are received, or until a timeout occurs.

PING6 server: 10.10.132.20
64 bytes from: 10.10.132.20: icmp_seq=0, time=0ms
64 bytes from: 10.10.132.20: icmp_seq=1, time=0ms
64 bytes from: 10.10.132.20: icmp_seq=2, time=0ms
64 bytes from: 10.10.132.20: icmp_seq=3, time=0ms
64 bytes from: 10.10.132.20: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
You can configure the following properties of the issued ICMP packets:

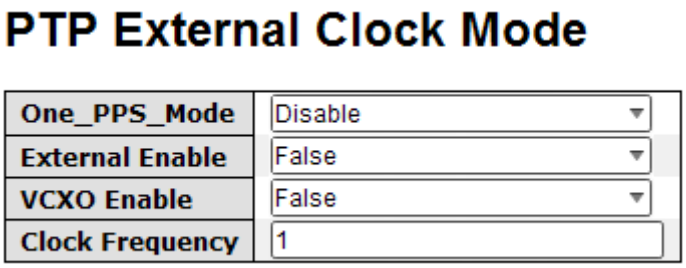
Label	Description
IP Address	The destination IP Address.
Ping Size	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

5.1.13 Synchronization-PTP

Overview of MAC-Based Authentication

This page allows the user to configure and inspect the current PTP clock settings.

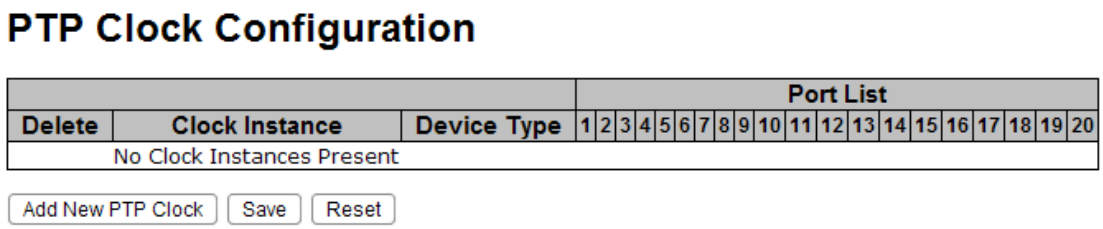
PTP External Clock Mode



Label	Description
One_pps_mode	This Selection box will allow you to select the One_pps_mode configuration. The following values are possible: 1. Output : Enable the 1 pps clock output 2. Input : Enable the 1 pps clock input 3. Disable : Disable the 1 pps clock in/out-put
External Enable	This Selection box will allow you to configure the External Clock

	output. The following values are possible: 1. True : Enable the external clock output 2. False : Disable the external clock output
VCXO_Enable	This Selection box will allow you to configure the External VCXO rate adjustment. The following values are possible: 1. True : Enable the external VCXO rate adjustment 2. False : Disable the external VCXO rate adjustment
Clock Frequency	This will allow the setting of the Clock Frequency. The possible range of values are 1 - 25000000 (1 - 25MHz)

PTP Clock Configuration


PTP Clock Configuration
Port List
Delete
Clock Instance
Device Type
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
No Clock Instances Present
Add New PTP Clock
Save
Reset

Label	Description
Delete	Check this box and click on 'Save' to delete the clock instance.
Clock Instance	Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to edit the Clock details.
Device Type	Indicates the Type of the Clock Instance. There are five Device Types. 1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock. 2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock. 3. E2e Transp - clock's Device Type is End to End Transparent Clock. 4. Master Only - clock's Device Type is Master Only. 5. Slave Only - clock's Device Type is Slave Only.
Port List	Set check mark for each port configured for this Clock Instance.
2 Step Flag	Static member: defined by the system, true if two-step Sync

	events and Pdelay_Resp events are used
Clock Identity	It shows unique clock identifier
One Way	If true, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.
Protocol	Transport protocol used by the PTP protocol engine ethernet PTP over Ethernet multicast ip4multi PTP over IPv4 multicast ip4uni PTP over IPv4 unicast Note : IPv4 unicast protocol only works in Master only and Slave only clocks See parameter Device Type In a unicast Slave only clock you also need configure which master clocks to request Announce and Sync messages from. See: Unicast Slave Configuration
VLAN Tag Enable	Enables the VLAN tagging for the PTP frames. Note: Packets are only tagged if the port is configured for vlan tagging. i.e: Port Type != Unaware and PortVLAN mode == None, and the port is member of the VLAN.
VID	VLAN Identifier used for tagging the PTP frames.
PCP	Priority Code Point value used for PTP frames.

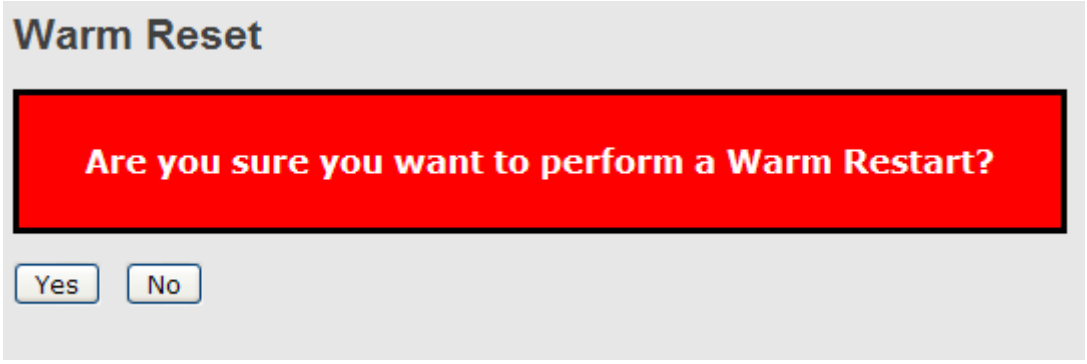
5.1.14 Factory Defaults

You can reset the configuration of the stack switch on this page. Only the IP configuration is retained.

Label	Description
Yes	Click to reset the configuration to Factory Defaults.
No	Click to return to the Port State page without resetting the configuration

5.1.15 System Reboot

You can reset the stack switch on this page. After reset, the system will boot normally as if you had powered-on the devices



Label	Description
Yes	Click to reboot device.
No	Click to return to the Port State page without rebooting.

Command Line Interface Management

6.1 About CLI Management

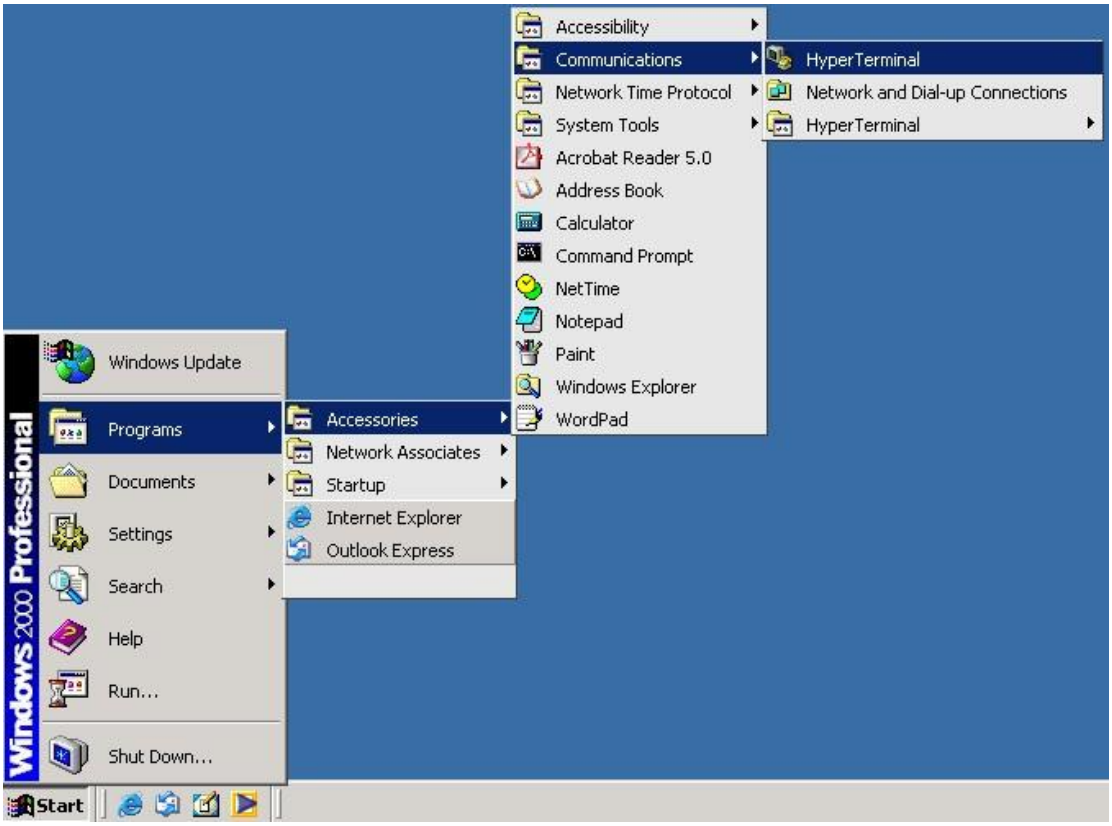
Besides a WEB-based management, the KY-4807EMX also supports CLI management. You can use console or telnet to management switch by CLI.

CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

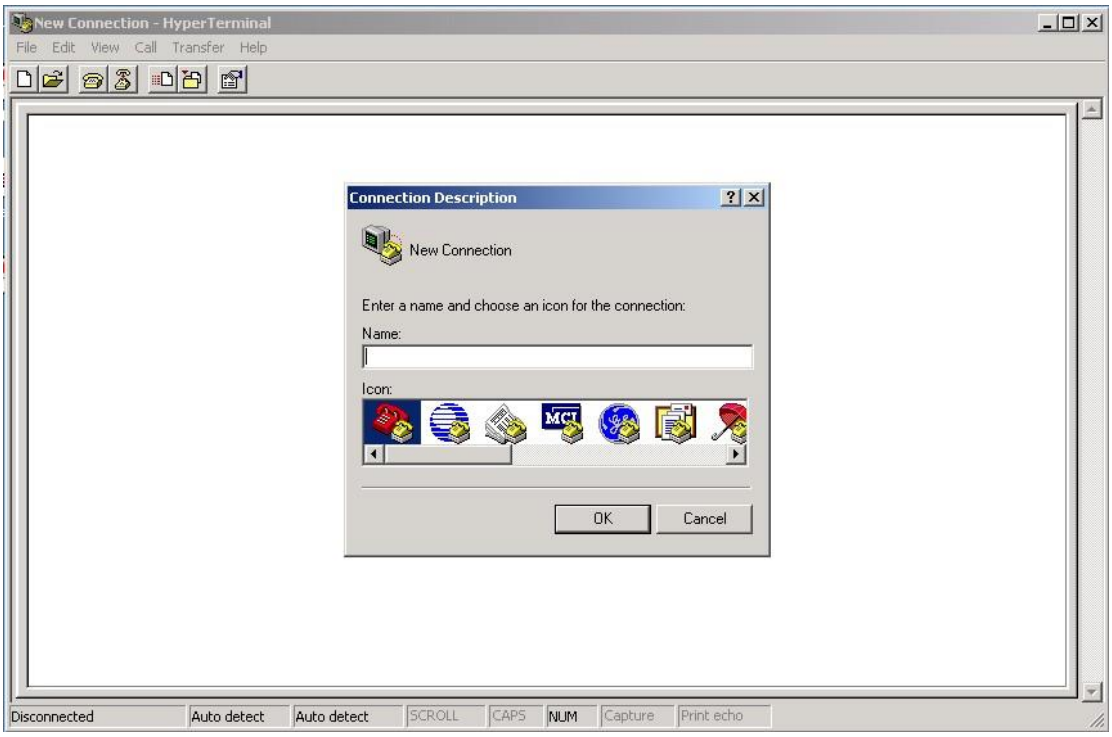
Before Configuring by RS-232 serial console, use an RJ45 to DB9-F cable to connect the Switches' RS-232 Console port to your PC's COM port.

Follow the steps below to access the console via RS-232 serial cable.

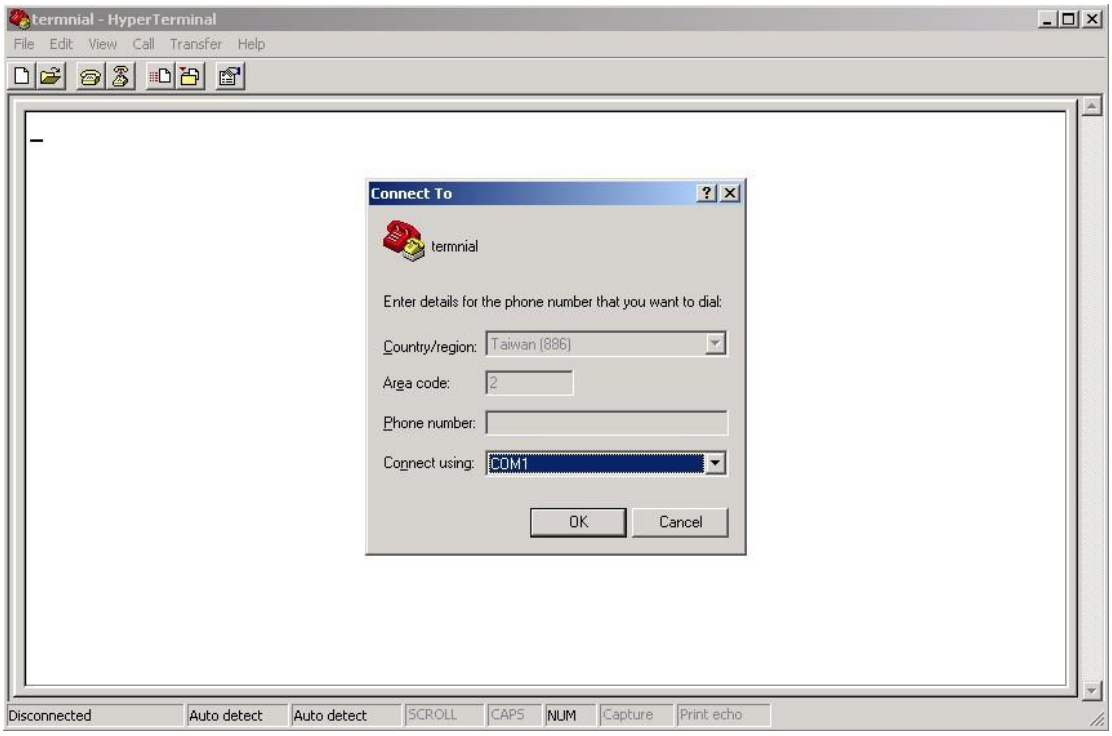
Step 1. From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal



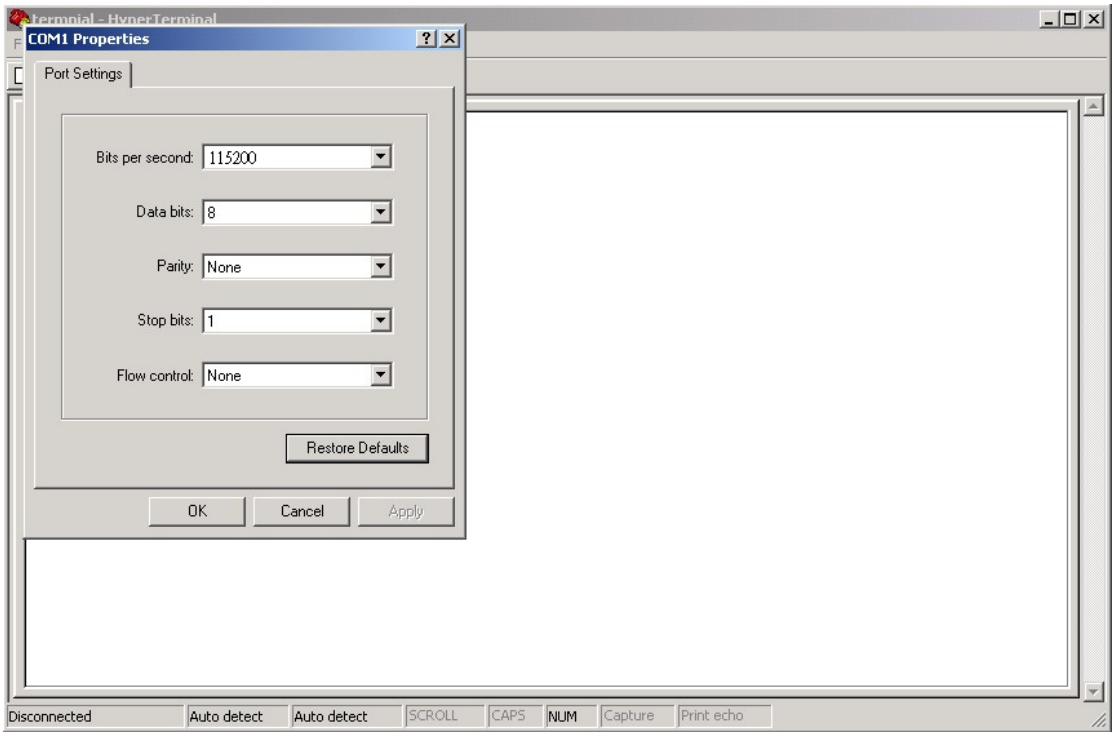
Step 2. Input a name for new connection



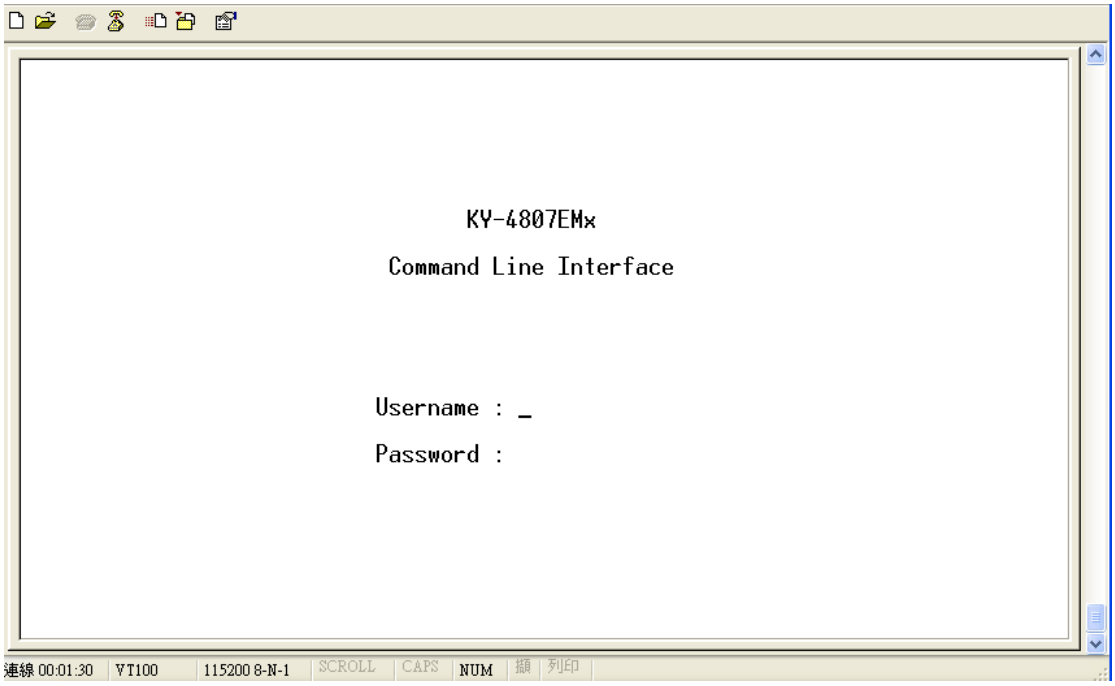
Step 3. Select to use COM port number



Step 4. The COM port properties setting, 115200 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.



Step 5. The Console login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), then press "**Enter**".



CLI Management by Telnet

Users can use "**TELNET**" to configure the switches.

The default value is as below:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

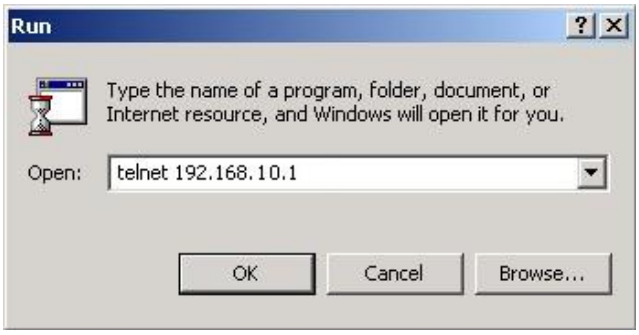
Default Gateway: **192.168.10.254**

User Name: **admin**

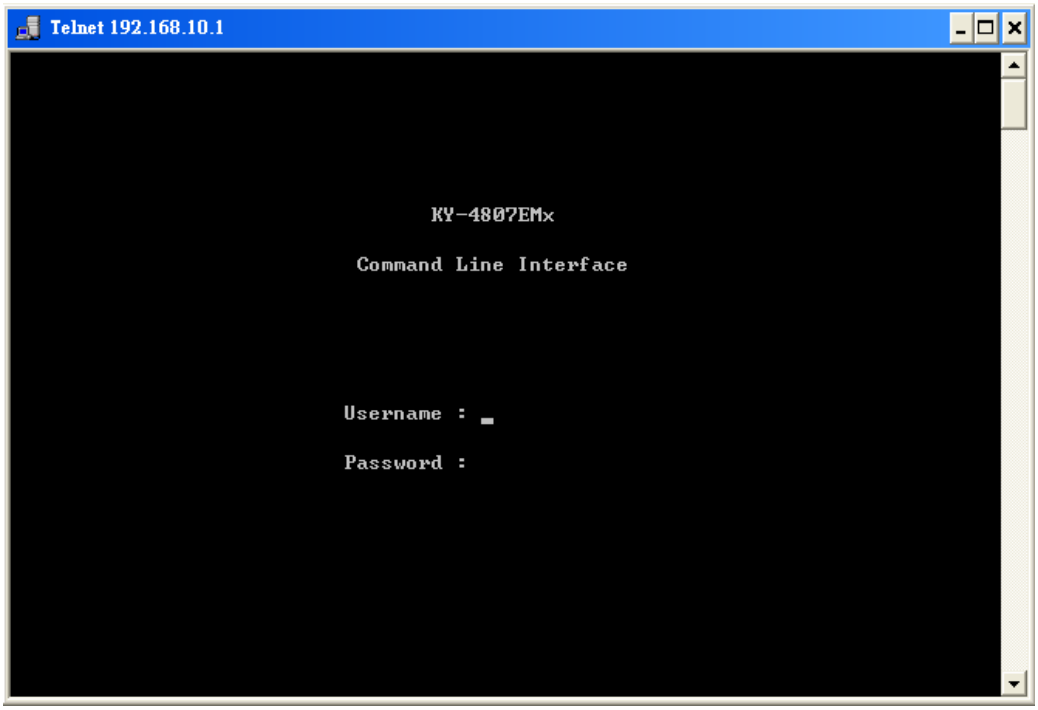
Password: **admin**

Follow the steps below to access the console via Telnet.

Step 1. Telnet to the IP address of the switch from the Windows "**Run**" command (or from the MS-DOS prompt) as below.



Step 2. The Login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), and then press "**Enter**"



Commander Groups

```
Command Groups:
---------------
System       : System settings and reset options
IP           : IP configuration and Ping
Port         : Port management
MAC          : MAC address table
VLAN         : Virtual LAN
PVLAN        : Private VLAN
Security     : Security management
STP          : Spanning Tree Protocol
Aggr         : Link Aggregation
LACP         : Link Aggregation Control Protocol
LLDP         : Link Layer Discovery Protocol
PoE          : Power Over Ethernet
QoS          : Quality of Service
Mirror       : Port mirroring
Config       : Load/Save of configuration via TFTP
Firmware     : Download of firmware via TFTP
PTP          : IEEE1588 Precision Time Protocol
Loop Protect : Loop Protection
IPMC         : MLD/IGMP Snooping
Fault        : Fault Alarm Configuration
Event        : Event Selection
DHCPServer   : DHCP Server Configuration
Ring         : Ring Configuration
Chain        : Chain Configuration
RCS          : Remote Control Security
Fastrecovery : Fast-Recovery Configuration
SFP          : SFP Monitor Configuration
DeviceBinding: Device Binding Configuration
MRP          : MRP Configuration
Modbus       : Modebus TCP Configuration
```

System

System>	Configuration [all] [<port list>]
	Reboot
	Restore Default [keep ip]
	Contact [<contact>]
	Name [<name>]
	Location [<location>]
	Description [<description>]
	Password <password>
	Username [<username>]
	Time zone [<offset>]
	Log [<log id>] [all | info | warning | error] [clear]

IP

IP>	Configuration
	DHCP [enable | disable]
	Setup [<ip addr>] [<ip mask>] [<ip router>] [<vid>]
	Ping <ip addr string> [<ping length>]
	SNTP [<ip addr string>]

Port

port>	Configuration [<port list>] [up | down]
	Mode [<port list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx|sfp_auto_ams]
	Flow Control [<port list>] [enable | disable]
	State [<port list>] [enable | disable]
	MaxFrame [<port_list>] [<max_frame>]
	Power [<port_list>] [enable|disable|actiphy|dynamic]
	Excessive [<port_list>] [discard|restart]
	Statistics [<port_list>] [<command>] [up|down]
	VeriPHY [<port_list>]
	SFP [<port_list>]

MAC

MAC>	Configuration [<port list>]
	Add <mac addr> <port list> [<vid>]
	Delete <mac addr> [<vid>]
	Lookup <mac addr> [<vid>]
	Age time [<age time>]
	Learning [<port list>] [auto | disable | secure]
	Dump [<mac max>] [<mac addr>] [<vid>]
	Statistics [<port list>]
	Flush

VLAN

VLAN>	Configuration [<port list>]
	PVID [<port_list>] [<vid>|none]
	Frame Type [<port list>] [all | tagged | untagged]
	Ingress Filter [<port list>] [enable | disable]
	tx_tag [<port_list>] [untag_pvid|untag_all|tag_all]
	Port Type [<port list>] [unaware |c-port | s-port | s-custom-port]
	Etype Custom Sport [<etype>]
	Add <vid>|<name> [<ports list>]
	Forbidden Add <vid>|<name> [<port list>]
	Delete <vid>|<name>
	Forbidden Delete <vid>|<name>
	Forbidden Lookup [<vid>] [(name <name>)]
	Lookup [<vid>] [(name <name>)] [combined | static | nas | all]
	Name Add <name> <vid>
	Name Delete <name>
	Name Lookup [<name>]
	Status [<port list>] [combined | static | nas | mstp | all | conflicts]

Private VLAN

PVLAN>	Configuration [<port list>]
	Add <pvlan id> [<port list>]
	Delete <pvlan id>
	Lookup [<pvlan id>]
	Isolate [<port_list>] [enable|disable]

Security

Security >	Switch	**Switch security setting**
	Network	**Network security setting**
	AAA	**Authentication, Authorization and Accounting setting**

Security Switch

Security/switch>	Password <password>
	Auth **Authentication**
	SSH **Secure Shell**
	HTTPS **Hypertext Transfer Protocol over Secure Socket Layer**
	RMON **Remote Network Monitor**

Security Switch Authentication

Security/switch/auth>	Configuration
	Method [console | telnet | ssh | web] [none | local | radius] [enable | disable]

Security Switch SSH

Security/switch/ssh>	Configuration
	Mode [enable | disable]

Security Switch HTTPS

Security/switch/ssh>	Configuration
	Mode [enable | disable]

Security Switch RMON

Security/switch/rmon>	Statistics Add <stats id> <data source>
	Statistics Delete <stats id>
	Statistics Lookup [<stats id>]
	History Add <history id> <data source> [<interval>] [<buckets>]
	History Delete <history id>
	History Lookup [<history id>]
	Alarm Add <alarm id> <interval> <alarm variable> [absolute | delta]<rising threshold> <rising event index> <falling threshold> <falling event index> [rising | falling | both]
	Alarm Delete <alarm id>
	Alarm Lookup [<alarm id>]

Security Network

Security/Network>	Psec	**Port Security Status**
	NAS	**Network Access Server (IEEE 802.1X)**
	ACL	**Access Control List**
	DHCP	**Dynamic Host Configuration Protocol**

Security Network Psec

Security/Network/Psec>	Switch [<port list>]
	Port [<port list>]

Security Network NAS

Security/Network/NAS>	Configuration [<port list>]
	Mode [enable | disable]
	State [<port list>] [auto | authorized | unauthorized | mac based]
	Re-authentication [enable | disable]
	Reauth Period [<reauth period>]
	EapolTimeout [<eapol_timeout>]
	Age time [<age time>]
	Hold time [<hold time>]
	Authenticate [<port list>] [now]
	Statistics [<port list>] [clear | eapol | radius]

Security Network ACL

Security/Network/ACL>	Configuration [<port list>]
	Action [<port list>] [permit | deny] [<rate limiter>][<port redirect>] [<mirror>] [<logging>] [<shutdown>]
	Policy [<port list>] [<policy>]
	Rate [<rate limiter list>] [<rate unit>] [<rate>]
	Add [<ace id>] [<ace id next>][(port <port list>)] [(policy <policy> <policy bitmask>)][<tagged>] [<vid>] [<tag prio>] [<dmac type>][(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp opcode>] [<arp flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp code>] [<ip flags>]) |

	(udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit | deny] [<rate limiter>] [<port redirect>] [<mirror>] [<logging>][<shutdown>]
	Delete <ace id>
	Lookup [<ace id>]
	Clear
	Status [combined | static | loop protect | dhcp | ptp | ipmc | conflicts]
	Port State [<port_list>] [enable|disable]

Security Network DHCP

Security/Network/DHCP>	Configuration
	Mode [enable | disable]
	Server [<ip addr>]
	Information Mode [enable | disable]
	Information Policy [replace | keep | drop]
	Statistics [clear]

Security Network AAA

Security/Network/AAA>	Configuration
	Timeout [<timeout>]
	Dead time [<dead time>]
	RADIUS [<server index>] [enable | disable] [<ip_addr string>] [<secret>] [<server port>]
	ACCT_RADIUS [<server index>] [enable | disable] [<ip addr string>] [<secret>] [<server port>]
	Statistics [<server index>]

STP

STP>	Configuration
	Version [<stp version>] Non-certified release, v
	Txhold [<hold count>]lt 15:15:15, Dec 6 2007

	Max Age [<max age>]
	Fwd Delay [<delay>]
	Bpdu Filter [enable | disable]
	Bpdu Guard [enable | disable]
	recovery [<timeout>]
	CName [<config-name>] [<integer>]
	Status [<msti>] [<port list>]
	Msti Priority [<msti>] [<priority>]
	Msti Map [<msti>] [clear]
	Msti Add <msti> <vid>
	Port Configuration [<port list>]
	Port Mode [<port_list>] [enable|disable]
	Port Edge [<port_list>] [enable|disable]
	Port AutoEdge [<port_list>] [enable|disable]
	Port P2P [<port_list>] [enable|disable|auto]
	Port RestrictedRole [<port_list>] [enable|disable]
	Port RestrictedTcn [<port_list>] [enable|disable]
	Port bpduGuard [<port_list>] [enable|disable]
	Port Statistics [<port list>]
	Port Mcheck [<port list>]
	Msti Port Configuration [<msti>] [<port_list>]
	MSTI Port Cost [<msti>] [<port list>] [<path cost>]
	MSTI Port Priority [<msti>] [<port list>] [<priority>]

Aggr

Aggr>	Configuration
	Add <port list> [<aggr_id>]
	Delete <aggr_id>
	Lookup [<aggr_id>]
	Mode [smac|dmac|ip|port] [enable|disable]

LACP

LACP>	Configuration [<port list>]
	Mode [<port_list>] [enable|disable]
	Key [<port list>] [<key>]

	Role [<port_list>] [active|passive]
	Status [<port list>]
	Statistics [<port list>] [clear]

LLDP

LLDP>	Configuration [<port list>]
	Mode [<port_list>] [enable|disable]
	Statistics [<port list>] [clear]
	Info [<port list>]

PoE

PoE>	Configuration [<port list>]
	Mode [<port_list>] [disabled|poe|poe+]
	Priority [<port list>] [low | high | critical]
	Mgmt mode [class con | class res | al con | al res | lldp res | lldp con]
	Maximum Power [<port list>] [<port power>]
	Status
	Primary Supply [<supply power>]

QoS

QoS>	DSCP Map [<dscp list>] [<class>] [<dpl>]
	DSCP Translation [<dscp list>] [<trans dscp>]
	DSCP Trust [<dscp list>] [enable | disable]
	DSCP Classification Mode [<dscp_list>] [enable|disable]
	DSCP Classification Map [<class list>] [<dpl_list>] [<dscp>]
	DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]
	Storm Unicast [enable | disable] [<packet rate>]
	Storm Multicast [enable | disable] [<packet rate>]
	Storm Broadcast [enable | disable] [<packet rate>]
	QCL Add [<qce_id>] [<qce_id_next>] [<port_list>] [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>] [(etype [<etype>]) | (LLC [<DSAP>] [<SSAP>] [<control>]) | (SNAP [<PID>]) |

	(ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) | (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])] [<class>] [<dp>] [<classified dscp>]
	QCL Delete <qce id>
	QCL Lookup [<qce id>]
	QCL Status [combined | static | conflicts]
	QCL Refresh

Mirror

Mirror>	Configuration [<port list>]
	Port [<port>|disable]
	Mode [<port_list>] [enable|disable|rx|tx]

Dot1x

Dot1x>	Configuration [<port list>]
	Mode [enable | disable]
	State [<port list>] [mac based | auto | authorized | unauthorized]
	Authenticate [<port list>] [now]
	Re-authentication [enable | disable]
	Period [<reauth period>]
	Timeout [<eapol timeout>]
	Statistics [<port list>] [clear | eapol | radius]
	Clients [<port_list>] [all|<client_cnt>]
	Age time [<age time>]
	Hold time [<hold time>]

IGMP

IGMP>	Configuration [<port list>]
	Mode [enable | disable]
	State [<vid>] [enable | disable]
	Querier [<vid>] [enable | disable]
	Fast leave [<port list>] [enable | disable]
	Router [<port_list>] [enable|disable]
	Flooding [enable | disable]
	Groups [<vid>]

	Status [<vid>]

ACL

ACL>	Configuration [<port list>]
	Action [<port list>] [permit | deny] [<rate limiter>] [<port copy>] [<logging>] [<shutdown>] Policy [<port list>] [<policy>]
	Rate [<rate limiter list>] [<packet rate>]
	Add [<ace id>] [<ace id next>] [switch | (port <port>) | (policy <policy>)] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) | (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) | (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) | (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) | (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) | (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])] [permit | deny] [<rate limiter>] [<port copy>] [<logging>] [<shutdown>] Delete <ace id>
	Lookup [<ace id>]
	Clear

Mirror

Mirror>	Configuration [<port list>]
	Port [<port>|disable]
	Mode [<port_list>] [enable|disable|rx|tx]

Configuration

Config>	Save <ip server> <filename>
	Load <ip server> <filename> [check]

Firmware

Firmware>	Load <ip addr string> <filename>

SNMP

SNMP>	Trap Inform Retry Times [<retries>]
	Trap Probe Security Engine ID [enable | disable]
	Trap Security Engine ID [<engineid>]
	Trap Security Name [<security name>]
	Engine ID [<engineid>]
	Community Add <community> [<ip_addr>] [<ip_mask>]
	Community Delete <index>
	Community Lookup [<index>]
	User Add <engineid> <user name> [MD5|SHA] [<auth password>] [DES] [<priv password>]
	User Delete <index>
	User Change key <engineid> <username> <auth password> [<priv password>]
	User Lookup [<index>]
	Group Add <security model> <security name> <group name>
	Group Delete <index>
	Group Lookup [<index>]
	View Add <view name> [included | excluded] <oid subtree>
	View Delete <index>
	View Lookup [<index>]
	Access Add <group name> <security model> <security level> [<read view name>] [<write view name>] Access Delete <index>
	Access Lookup [<index>]

Firmware

Firmware>	Load <ip addr string> <file name>

PTP

PTP>	Configuration [<clockinst>]
	Port State <clockinst> [<port list>] [enable | disable | internal]
	Clock Create <clockinst> [<devtype>] [<twostep>] [<protocol>] [<oneway>]

	[<clockid>] [<tag_enable>] [<vid>] [<prio>]
	Clock Delete <clockinst> [<devtype>]
	Default DS <clockinst> [<priority1>] [<priority2>] [<domain>]
	Current DS <clockinst>
	Parent DS <clockinst>
	Timing Properties <clockinst> [<utcoffset>] [<valid>] [<leap59>] [<leap61>] [<timetrac>] [<freqtrac>] [<ptptimescale>] [<timesource>]
	PTP Port Data Set <clockinst> [<port list>] [<announceintv>] [<announceto>] [<syncintv>] [<delaymech>] [<minpdelayreqintv>] [<delay asymmetry>] [<ingress Latency>]
	Local Clock <clockinst> [update | show | ratio] [<clockratio>]
	Filter <clockinst> [<def_delay_filt>] [<period>] [<dist>]
	Servo <clockinst> [<display states>] [<ap_enable>] [<ai_enable>] [<ad_enable>] [<ap>] [<ai>] [<ad>]
	Slave Table Unicast <clockinst>
	Uni Config <clockinst> [<index>] [<duration>] [<ip_addr>]
	Foreign Masters <clockinst> [<port list>]
	Egress Latency [show | clear]
	Master Table Unicast <clock inst>
	Ext Clock Mode [<one pps mode>] [<ext enable>] [<clockfreq>] [<vcxo_enable>]
	One Pps Action [<one pps clear>]
	Debug Mode <clockinst> [<debug mode>]
	Wireless mode <clockinst> [<port list>] [enable | disable]
	Wireless pre notification <clockinst> <port list>
	Wireless delay <clockinst> [<port list>] [<base delay>] [<incr delay>]

Loop Protect

Loop Protect>	Configuration
	Mode [enable | disable]
	Transmit [<transmit-time>]
	Shutdown [<shutdown-time>]
	Port Configuration [<port list>]
	Port Mode [<port_list>] [enable|disable]
	Port Action [<port_list>] [shutdown|shut_log|log]
	Port Transmit [<port_list>] [enable|disable]

	Status [<port list>]

IPMC

IPMC>	Configuration [igmp]
	Mode [igmp] [enable | disable]
	Flooding [igmp] [enable | disable]
	VLAN Add [igmp] <vid>
	VLAN Delete [igmp] <vid>
	State [igmp] [<vid>] [enable | disable]
	Querier [igmp] [<vid>] [enable | disable]
	Fast Leave [igmp] [<port_list>] [enable | disable]
	Router [igmp] [<port_list>] [enable|disable]
	Status [igmp] [<vid>]
	Groups [igmp] [<vid>]
	Version [igmp] [<vid>]

Fault

Fault>	Alarm Port Link Down [<port list>] [enable | disable]
	Alarm Power Failure [pwr1|pwr2|pwr3] [enable | disable]

Event

Event>	Configuration
	Syslog System Start [enable | disable]
	Syslog Power Status [enable | disable]
	Syslog SNMP Authentication Failure [enable | disable]
	Syslog Ring Topology Change [enable | disable]
	Syslog Port [<port list>] [disable | linkup | link down | both]
	SMTP System Start [enable | disable]
	SMTP Power Status [enable | disable]
	SMTP SNMP Authentication Failure [enable | disable]
	SMTP Ring Topology Change [enable | disable]
	SMTP Port [<port list>] [disable |linkup |link down | both]

DHCP Server

DHCP Server>	Mode [enable | disable]

	Setup [<ip start>] [<ip end>] [<ip mask>] [<ip router>] [<ip dns>] [<ip tftp>] [<lease>] [<boot file>]

Ring

Ring>	Mode [enable | disable]
	Master [enable | disable]
	1stRingPort [<port>]
	2ndRingPort [<port>]
	Couple Mode [enable | disable]
	Couple Port [<port>]
	Dual homing Mode [enable | disable]
	Dual homing Port [<port>]

Chain

Chain>	Configuration
	Mode [enable | disable]
	1stUplinkPort [<port>]
	2ndUplinkPort [<port>]
	Edge Port [1st | 2nd | none]

RCS

RCS>	Mode [enable | disable]
	Add [<ip addr>] [<port list>] [web on | web off] [telnet on | telnet off] [snmp on | snmp off]
	Del <index>
	Configuration

Fast Recovery

Fast Recovery>	Mode [enable | disable]
	Port [<port_list>] [<fr_priority>]

SFP

SFP>	syslog [enable | disable]
	temp [<temperature>]

	Info

Device Binding

Device Binding>	Mode [enable | disable]
	Port Mode [<port_list>] [disable|scan|binding|shutdown]
	Port DDOS Mode [<port_list>] [enable|disable]
	Port DDOS Sensibility [<port list>] [low | normal | medium | high]
	Port DDOS Packet [<port list>] [rx total | rx unicast | rx multicast| rx broadcast | tcp | udp]
	Port DDOS Low [<port list>] [<socket number>]
	Port DDOS High [<port list>] [<socket number>]
	Port DDOS Filter [<port_list>] [source|destination]
	Port DDOS Action [<port list>] [do_nothing|block_1_min|block_10_mins|block|shutdown|only_log|reboot_device]
	Port DDOS Status [<port_list>]
	Port Alive Mode [<port_list>] [enable|disable]
	Port Alive Action [<port list>] [do-nothing | link change | shutdown |only log | reboot device]
	Port Alive Status [<port_list>]
	Port Stream Mode [<port_list>] [enable|disable]
	Port Stream Action [<port list>] [do-nothing |only_log]
	Port Stream Status [<port list>]
	Port Addr [<port list>] [<ip addr>] [<mac addr>]
	Port Alias [<port_list>] [<ip_addr>]
	Port DeviceType [<port_list>] [unknown|ip_cam|ip_phone|ap|pc|plc|nvr]
	Port Location [<port_list>] [<device_location>]
	Port Description [<port_list>] [<device_description>]

MRP

MRP>	Configuration
	Mode [enable | disable]
	Manager [enable | disable]
	React [enable | disable]
	1stRingPort [<mrp port>]
	2ndRingPort [<mrp port>]

	Parameter MRP_TOPchgT [<value>]
	Parameter MRP_TOPNRmax [<value>]
	Parameter MRP_TSTshortT [<value>]
	Parameter MRP_TSTdefaultT [<value>]
	Parameter MRP_TSTNRmax [<value>]
	Parameter MRP_LNKdownT [<value>]
	Parameter MRP_LNKupT [<value>]
	Parameter MRP_LNKNRmax [<value>]

Modbus

Modbus>	Status
	Mode [enable | disable]

Technical Specifications

Kyland-USA Model	KY-4807EMx
Physical Ports	
10/100/1000Base-T(X) Ports in RJ45 Auto MDI/MDIX	**8**
100/1000Base-X with SFP port	**12**
Technology	
Ethernet Standards	IEEE 802.3 for 10Base-T IEEE 802.3u for 100Base-TX and 100Base-FX IEEE 802.3ab for 1000Base-T IEEE 802.z for 1000Base-X IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol) IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)
MAC Table	12k
Pr ority Queues	8
Processing	Store-and-Forward
Switch Properties	Switching latency: 6 us Switching bandwidth: 40Gbps Max. Number of Available VLANs: 256 IGMP multicast groups: 128 for each VLAN Port rate lim ting: User Define
Jumbo frame	Up to 9.6K Bytes
Secur ty Features	Device Binding security feature Enable/disable ports, MAC based port security Port based network access control (802.1x) VLAN (802.1Q) to segregate and secure network traff c Radius centralized password management SNMPv3 encrypted authentication and access security Https / SSH enhance network security
Software Features	STP/RSTP/MSTP (IEEE 802.1D/w/s) Redundant Ring (O-Ring) with recovery time less than 30ms over 250 units TOS/DiffServ supported Quality of Service (802.1p) for real-time traffic VLAN (802.1Q) with VLAN tagging and GVRP supported IGMP Snooping IP-based bandw dth management Application-based QoS management DOS/DDOS auto prevention Port configurat on, status, statistics, mon toring, security DHCP Server/Client/Relay SMTP Client Modbus TCP
Network Redundancy	Ring Open-Ring Chain MRP MSTP (RSTP/STP compatible)
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable. 115200bps, 8, N, 1
LED indicators	
Power Ind cator (PWR)	Green : Power LED x 2
Ring Master Indicator (R.M.)	Green : Indicates that the system is operating in Ringmaster mode
RingIndicator (Ring)	Green : Indicates that the system operating in Ring mode

	Green Blinking: Indicates that the Ring is broken.
Fault Indicator (Fault)	Amber : Indicate unexpected event occurred
10/100/1000Base-T(X) RJ45 Port Ind cator	Green for 1000Mbps Link/Act indicator. Amber for duplex indicator
100/1000Base-X SFP Port Indicator	Green for port Link/Act.
Fault contact	
Relay	Relay output to carry capacity of 1A at 24VDC
Power	
Redundant Input power	Dual DC inputs. 12~48VDC on 6-pin terminal block
Power consumption (Typ.)	<10 Watts
Overload current protection	Present
Reverse Polarity Protection	Present
Physical Characteristic	
Enclosure	IP-30
Dimension (W x D x H)	96.4 (W) x 105.5 (D) x 154 (H) mm (3.8 x 4.15 x 6.06 inch)
Weight (g)	1210 g
Environmental	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	-40 to 85°C (-40 to 185°F)
Operating Humid ty	5% to 97% Non-condensing
Regulatory approvals	
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD) EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1
Warranty	5 years